



Informatics

# Assessing Service Management Strategies for Complex IT Systems in the Financial Sector

## Monitoring, Automation, and Modernization in Business Environments

DIPLOMA THESIS

submitted in partial fulfillment of the requirements for the degree of

**Diplom-Ingenieur**

in

**Business Informatics**

by

**Tobias Gösslbauer**

Registration Number 11909912

to the Faculty of Informatics

at the TU Wien

Advisor: Privatdoz. Dipl.-Ing. Mag.rer.soc.oec. Dr.techn. Edgar Weippl

Assistance: Univ.Lektor Dipl.-Ing. Dr.techn. Alexander Schatten

Vienna, October 13, 2025

\_\_\_\_\_  
Tobias Gösslbauer

\_\_\_\_\_  
Edgar Weippl

# Erklärung zur Verfassung der Arbeit

Tobias Gösslbauer

Hiermit erkläre ich, dass ich diese Arbeit selbständig verfasst habe, dass ich die verwendeten Quellen und Hilfsmittel vollständig angegeben habe und dass ich die Stellen der Arbeit – einschließlich Tabellen, Karten und Abbildungen –, die anderen Werken oder dem Internet im Wortlaut oder dem Sinn nach entnommen sind, auf jeden Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht habe.

Wien, 13. Oktober 2025

---

Tobias Gösslbauer

# Abstract

This thesis explores which service management strategies are best adapted to meet the demands of complex Information Technology (IT) systems within the financial sector. It focuses on identifying practical approaches to effectively manage complexity drivers and aims to understand how financial institutions adapt their service management practices to increasing IT complexity. A twofold methodology was employed: a literature review that establishes the theoretical foundation, and semi-structured interviews with senior professionals from various financial institutions. The findings reveal that traditional service management strategies prove to not effectively manage complex IT systems. Emerging strategies include selective automation, context-aware Key Performance Indicator (KPI) design with clear ownership, feedback-driven service enhancement, and adaptive monitoring practices. Furthermore, continuous monitoring and the use of operational data to improve the service delivery were identified as critical success factors. The changing system states necessitate proactive adaptation. These results imply that service management in complex systems calls for a system design that is context-aware and embraces unpredictability. The insights contribute to bridging complexity theory and IT Service Management (ITSM), offering insights for the academic discourse and providing practical guidance for practitioners.

# Contents

<b>Abstract</b>	<b>iii</b>
<b>Contents</b>	<b>iv</b>
<b>1 Introduction</b>	<b>1</b>
1.1 Problem Description . . . . .	1
1.2 Research Objectives and Questions . . . . .	2
<b>2 Methodological Approach</b>	<b>4</b>
2.1 Systematic Literature Review . . . . .	4
2.2 Semi-Structured Expert Interviews (Qualitative Research) . . . . .	6
<b>3 Foundations of Complex Systems</b>	<b>12</b>
3.1 Introduction to Complex Systems . . . . .	12
3.2 Foundations of Complexity Theory . . . . .	13
3.3 Applications Across Domains . . . . .	16
<b>4 Managing Complex Systems</b>	<b>19</b>
4.1 Introduction . . . . .	19
4.2 Principles of Management in Complex Systems . . . . .	19
4.3 Objectives and Properties of Managing Complex Systems . . . . .	21
4.4 Frameworks and Models for Managing Complex Systems . . . . .	22
4.5 Challenges in Managing Complex Systems . . . . .	24
4.6 Applications in Complex Systems . . . . .	25
<b>5 Complex IT Systems: Foundations and Challenges</b>	<b>27</b>
5.1 Introduction . . . . .	27
5.2 Evolution of IT Systems Toward Complexity . . . . .	28
5.3 Defining Complex IT Systems . . . . .	30
5.4 Complexity in ITSM . . . . .	34
5.5 Challenges in Managing Complex IT Systems . . . . .	38
5.6 Conclusion . . . . .	42

<b>6</b>	<b>Service Management Strategies for Complex IT Systems in the Financial Sector</b>	<b>44</b>
6.1	Introduction . . . . .	44
6.2	Impact of Increasing IT Complexity on Service Management Practices	45
6.3	Demarcation of Service Management Responsibilities in Complex Environments . . . . .	47
6.4	Strategies and Methods for Managing Service Delivery in Complex IT Environments . . . . .	52
6.5	Assessing the Effectiveness of Service Management in Financial Institutions	59
6.6	Preliminary Reflections and Synthesis . . . . .	64
<b>7</b>	<b>Interviews</b>	<b>67</b>
7.1	Introduction . . . . .	67
7.2	Interview Overview . . . . .	67
7.3	Emerging Themes . . . . .	70
<b>8</b>	<b>Discussion</b>	<b>78</b>
8.1	Introduction . . . . .	78
8.2	RQ1: How do businesses in the financial sector measure the success of service management practices in complex IT systems, and what metrics or indicators are used? . . . . .	78
8.3	RQ2: How do stakeholders in financial institutions evaluate the effectiveness of service management metrics in complex IT environments? . . . . .	81
8.4	RQ3: What role do automation and monitoring tools play in managing service delivery in complex IT systems, and to what extent are their benefits and limitations observed? . . . . .	83
8.5	RQ4: What specific service management strategies are adapted by businesses in the financial sector to handle the increasing complexity and interdependencies of modern IT systems? . . . . .	86
8.6	Strengths and Research Contributions . . . . .	88
8.7	Limitations and Critical Reflection . . . . .	89
<b>9</b>	<b>Conclusion</b>	<b>91</b>
	<b>Bibliography</b>	<b>111</b>

# Introduction

## 1.1 Problem Description

In our evolving world, complex IT systems have become increasingly pervasive across various domains, particularly in service management in the financial sector. Traditionally, IT systems used to be primarily self-contained, operating independently within well-defined boundaries and interactions between themselves [52]. However, as the demands for connectivity, scalability, and functionality have grown, these systems evolved into highly interconnected and dynamic environments with various integrated components such as cloud infrastructures, microservices, and distributed networks.

Complex IT systems are characterized by a high degree of interdependence between components, where the behavior of the whole system cannot be easily predicted from individual parts and their processes. These systems often exhibit unanticipated behaviors that result from the interactions between components. In turn, this complicates management, ultimately necessitating broader perspectives to effectively oversee and control these complex systems [108]. As systems become more complex, traditional management methods, which worked well for simpler, contained systems, start to lose their effectiveness [40].

In order to comprehend large IT systems, it is necessary to take into account different factors [52]. Differences between systems can be found in how they handle data, process tasks, and scale to meet user demands. For example, cloud-based systems may prioritize flexibility and scalability, while distributed systems might focus on redundancy and fault tolerance. Distinctions help to categorize and understand the unique challenges of managing different types of complex IT systems.

The increasing complexity of IT systems in the financial sector introduced new challenges for service management, particularly in ensuring reliability, resilience, and effectiveness [28]. Traditional IT management frameworks, designed for more predictable and self-

contained systems, struggle to accommodate the high degree of interdependence and emergent behaviors found in modern infrastructures. Prior research by Tian and Kaur [110] and Sommerville et al. [104] has identified limitations in existing service management methodologies when applied to complex IT environments. One of the primary limitations is the lack of structured frameworks to measure the success and effectiveness of service management approaches in complex IT systems, particularly in dynamic and high-risk sectors such as finance. Overall, a systematic understanding of how specific service management strategies perform in complex systems remains underexplored. This research aims to address this gap by analyzing the extent to which different management approaches impact key performance factors such as system reliability, fault tolerance, and adaptability.

## 1.2 Research Objectives and Questions

The goal of this thesis is to depict effective service management strategies tailored specifically for complex IT systems in the financial sector. To ensure an accurate representation of the current service management strategies, interviews will be conducted with individuals working in the financial or service management sector. Through this perspective, the aim is to highlight the distinguishing features that make the service management of complex systems more demanding, as well as identify potential strategies to manage these difficulties. By providing practical examples from leaders in business environments, a comprehensive understanding of complex IT systems can be developed. Examples such as the differences between a standalone enterprise system and a distributed, cloud-based system will demonstrate how these distinctions necessitate a shift in service management strategies. Similar, the contrast between non-complex systems' reliance on linear, predictable workflows and complex systems' unpredictable dynamic behaviors will be further examined. These interviews can assist to uncover best practices and creative approaches to administering such systems, as well as offer insightful information on the difficulties encountered in real-world scenarios. To improve comprehension of how theory becomes practice, the results of these interviews will be incorporated into the thesis.

Furthermore, the strategies that identify and address the emergent behaviors inherent in complex environments, as well as the usage of automation and monitoring techniques, will also be explored. In addition, the thesis acknowledges service reliability challenges and amplifies the risk of security vulnerabilities with the increase of complexity. Hence, effective service management is essential to ensure security and maintain oversight. Analyzing service management and its shortcomings when applied to complex systems will be involved, as well as modernization approaches. Since the research field of complex systems is still small compared to other fields, possible alternative methods found in the literature will be considered that leverage adaptive, emergent approaches to enhance control and efficiency.

The central Research Question (RQ)s guiding this thesis are:

- **RQ1:** How do businesses in the financial sector measure the success of service

management practices in complex IT systems, and what metrics or indicators are used?

- **RQ2:** How do stakeholders in financial institutions evaluate the effectiveness of service management metrics in complex IT environments?
- **RQ3:** What role do automation and monitoring tools play in managing service delivery in complex IT systems, and to what extent are their benefits and limitations observed?
- **RQ4:** What specific service management strategies are adapted by businesses in the financial sector to handle the increasing complexity and interdependencies of modern IT systems?

By answering these questions and combining theoretical research with practical insights from interviews, this thesis aims to provide actionable recommendations for IT managers, equipping them with service management strategies needed to better manage and control increasingly complex IT environments. In addition, this thesis aims to enhance and contribute to previous research analyzing management practices in the context of complex IT systems.

This thesis excludes certain aspects that, while relevant to service management in complex IT systems, fall outside its primary focus. For example, legal and regulatory compliance issues, such as data protection laws, cybersecurity regulations, and contractual obligations, are not explored in depth, as the focus is on operational and strategic service management practices rather than on legal frameworks. Additionally, this study does not delve into specific industry standards or certifications (e.g., ISO/IEC standards), nor does it cover the financial implications or cost-benefit analyzes of implementing different service management strategies. The emphasis remains on identifying adaptive approaches to service management that address the unique challenges of complex IT environments. Thus, the findings and recommendations are primarily aimed at practical and operational improvements rather than encompassing the full regulatory and financial landscape of IT management, as well as the historical aspect of such systems.

# Methodological Approach

This thesis adopts a two-pronged methodological approach to systematically explore management and control approaches for complex IT systems. It integrates a systematic literature review and semi-structured expert interviews as part of a qualitative research framework.

## 2.1 Systematic Literature Review

The systematic literature review synthesizes foundational knowledge from existing research, following the methodology outlined by Webster and Watson [115] and Kitchenham and Charters [62]. Both emphasize a structured approach comprising the following steps:

1. Defining RQs as stated in section 1.2
2. Develop Search Strategy  
A search strategy is constructed to locate relevant studies in prominent academic databases. In this thesis, the primary databases are:
  - IEEE Xplore
  - ACM Digital Library
  - SpringerLink

The search was primarily limited to peer-reviewed journal articles and conference proceedings, while also including other forms of scholarly literature where relevant, with a focus on more recent publications, ensured that findings were relevant to modern IT environments.

### 3. Construct Search Strings

Based on the defined RQs and initial exploratory reading, the following key concepts and synonyms have been identified:

- Financial sector context: (*“IT Infrastructure in Financial Services” OR “Financial Technology (FinTech) Ecosystem” OR “Core Banking Systems” OR “Financial System Architecture”*)
- Complexity/Complex systems: (*“Complex Systems” OR “Managing Complexity” OR “Complex Systems Foundation”*)
- ITSM: (*“Service Management” OR “IT Operations” OR “Management of Complex Systems”*)
- Characteristics or Challenges: (*“Emergent behavior” OR “Interdependencies” OR “Resilience”*)

Example of a combined Boolean search string could be:

( (*“IT Infrastructure in Financial Services” OR “FinTech Ecosystem” OR “Core Banking Systems” OR “Financial System Architecture”*)  
 AND (*“Complex Systems” OR “Managing Complexity” OR “Complex Systems Foundation”*)  
 AND (*“Service Management” OR “IT Operations” OR “Management of Complex Systems”*)  
 AND (*“Emergent behavior” OR “Interdependencies” OR “Resilience”*) )

Multiple variations of these terms and synonyms were tested to capture a broad range of relevant literature.

### 4. Apply Inclusion and Exclusion Criteria

After retrieving the initial set of articles, a multi-stage screening process was conducted:

- Title/Abstract Screening: Eliminate articles that do not address management strategies, ITSM, complexity or the financial domain.
- Full-Text Review: Include papers that:
  - Primarily focus on IT systems in finance (e.g. commercial banking, FinTech, core banking infrastructures).
  - Present explicit service management or operational strategies for complex IT.
  - Provide methodological rigor or empirical evidence.
- Exclude papers that:
  - Lack a clear methodology or relevant context.
  - Focus solely on unrelated technical aspects
  - Are not peer-reviewed (e.g., blog posts, non-reviewed white papers).

### 5. Data Extraction and Synthesis

A standardized extraction process gathered key data from each selected study, such as:

- Publication details (authors, title, venue, year).
- Domain focus (e.g., retail banking, investment banking, FinTech startups).
- Main findings on service management, complexity, and resilience.
- Reported frameworks or solutions for managing complex systems in finance.

In this review, the attention was on service management strategies in complex IT systems, focusing on effectiveness, reliability, and resilience. Structured methods and iterative refinement improved the accuracy in these domains. Through the iterative feedback-based approach the clustering of findings into thematic areas such as “automation,” “legacy system,” and “monitoring” were established. These clusters formed a theoretical foundation for the subsequent interviews.

Studies that do not focus on IT systems or lack a clear methodology were excluded. This procedure guaranteed the findings’ applicability and relevance, especially when it comes to determining the areas where conventional methods fall short and adaptive tactics are required.

## 2.2 Semi-Structured Expert Interviews (Qualitative Research)

Expert interviews were used in this research to give contextual insights from the literature review. These interviews provided expert perspectives on the topic, thus complementing other research steps.

### 2.2.1 Framework Development

Establishing a clear framework was critical before conducting interviews. Both Cooke and McDonald [36] and Bogner, Littig, and Menz [23] provide such a framework with an emphasis on structured methodologies to enhance the accuracy and depth of expert input. While Cooke and McDonald [36] highlight cognitive psychology with elicitation techniques to minimize inaccuracies stemming from introspection, Bogner, Littig, and Menz [23] write about the necessity of multiple knowledge acquisition techniques such as structured interviews, observation, and protocol analysis to reduce bias and improve reliability.

Theory-generating expert interviews, as advocated by Bogner, Littig, and Menz [23], are particularly useful in complex research areas where existing theories may be insufficient. These interviews, in addition to the gathered information, also promote reflection. By fostering a reciprocal dialog and flexibility in questioning, interviewees can elaborate on unforeseen but critical issues.

The planning and execution of semi-structured interviews requires careful consideration. Hove and Anda [55] identify key areas, including effort estimation, interviewer qualifications, interaction fostering, and tool selection, to ensure reliable results. Similarly, Saldaña [98] emphasizes the interviewer is considered a “human instrument” to the qualitative research, necessitating adaptability during the interview process, similar to Bogner, Littig, and Menz [23].

Iterative development of the interviews, as proposed by Bogner, Littig, and Menz [23] ensures comprehensive topic coverage while allowing flexibility for emergent themes. Iterative expert-interviews methodology begins with broad themes, which are refined through pilot interviews or multiple rounds, thereby improving the overall validity of the collected data.

Building on these principles, the proposed framework defines key themes, interview formats, and potential variations. It also incorporates indirect elicitation methods to reduce the cognitive load on experts, ensuring reliable data collection. This suggests that structured scenarios can improve the precision of expert judgments by providing a consistent context for responses.

### 2.2.2 Interview Process

The interview process, as outlined by Hove and Anda [55] and Cooke and McDonald [36], involves multiple steps to maximize the potential information and consistency. While Hove and Anda [55] focus on logistical aspects such as scheduling, preparing an interview guide, conducting interviews, and transcribing data, Cooke and McDonald [36] suggests to use of structured tasks to elicit both procedural and declarative knowledge. Incorporating scaling techniques further enhances the reliability of knowledge representation.

To gain deeper insights, additional interviewing techniques, such as repertory grids and card sorting are recommended by Eriksson [41] and were employed where appropriate. These methods allow for a systematic analysis of expert input, revealing nuanced perspectives that might otherwise be overlooked.

The type of interview conducted depends on the research objective. Bogner, Littig, and Menz [23] categorize interviews into exploratory, systematizing, and theory-generating types. Using a semi-structured approach that strikes a balance between consistency and flexibility allows more detail about subjects while maintaining a logical structure. In order to increase data richness, narrative prompts were used to provide thorough contextual descriptions.

Mergel, Edelmann, and Haug [77] emphasize logistical considerations about the general interview, examples are reliable recording equipment and familiarity with participants’ backgrounds. This preparatory work helps build rapport and improves the quality of collected data. Additionally, pilot interviews, as suggested by Hove and Anda [55], were conducted in advance to refine the guide and enhance interviewer competence.

To ensure a representative and reliable sample, Christopoulos [32] propose the Peer Esteem Snowballing (PEST) technique. PEST reduces selection bias and guarantees wide expert participation by fusing network analysis with iterative nomination waves. This technique was adapted to this case to ensure diverse opinions while maintaining high relevance to the RQ.

### 2.2.3 Problem Statement & Interview Types

Eriksson [41] and Bogner, Littig, and Menz [23] categorize interview types based on different research objectives, distinguishing between tutorial, structured, exploratory, and theory-generating approaches.

Interview Type	Description	Source
Tutorial	Experts introduce the domain, providing foundational knowledge.	Eriksson [41]
Focused	Prepares broad topics without detailed questions, allowing exploration.	Eriksson [41]
Structured	Involves detailed, in-depth questions to gather specific, consistent information.	Eriksson [41]
Teachback	Experts explain processes, and the interviewer reiterates them for validation.	Eriksson [41]
Exploratory	Aims to gain a broad understanding of a subject in an open-ended manner.	Bogner, Littig, and Menz [23]
Systematizing	Focuses on gathering structured knowledge for detailed representations.	Bogner, Littig, and Menz [23]
Theory-Generating	Aims to develop new theoretical frameworks based on expert input.	Bogner, Littig, and Menz [23]

Table 2.1: Interview Types with Descriptions and Sources

An introduction had to be given to describe the problem to the interviewee after that a semi-structured interview approach, combining open-ended questions with a flexible structure allowed experts to elaborate on key topics, providing richer insights. Bogner, Littig, and Menz [23] emphasize the importance of narrative-driven semi-structured interviews, which enabled to sharing of detailed experiential knowledge. Including open-ended, probing, and follow-up questions ensures breadth and depth of information gathering.

To enhance the depth of the qualitative research, it is also crucial to consider how the choice of interview type influences data validity and reliability. Saldaña [98] highlights that selecting the appropriate interview type and questions for each participant requires careful consideration. For instance, exploratory interviews are particularly useful during the initial phases of research when broad insights are needed, while structured interviews are better suited for later stages requiring precise, replicable data. Additionally, combining different interview types can provide a well-rounded perspective on the problem. This semi-structured approach ensures both breadth and depth in the findings by striking a balance between open-ended discovery and thorough verification.

### 2.2.4 Expert Selection

Effective expert selection uses criteria to find the right interviewees. Li and Smidts [65] recommend including credibility (experience and expertise in the domain), knowledgeability (depth of subject knowledge), and dependability (willingness to participate) as criteria.

This thesis follows a purposive sampling strategy, ensuring participants are directly relevant to the research objectives. A snowball sampling approach was also used, where initial experts nominate additional participants, broadening the sample pool and enhancing representation. The PEST technique proposes this by identifying well-regarded professionals through network analysis. This thereby improves the reliability and representativeness of the sample by expanding it iteratively through peer nominations [32]. According to Mergel, Edelmann, and Haug [77], this is a purposeful technique that guarantees the inclusion of various and pertinent expert viewpoints.

To mitigate bias, Cooke and McDonald [36] and Eriksson [41] stress the importance of involving experts from varied backgrounds. In line with this, the selected experts represented different sectors, such as financial services, IT consulting, and operational management, ensuring a comprehensive range of views. Additionally, the experts were selected from different positions within these companies.

Bogner, Littig, and Menz [23] highlight that selected experts should not only possess domain expertise but also strong communication skills to provide in-depth, reflective insights. Purposive sampling ensures that participants meet these criteria. Saldaña [98] underscores the importance of selecting individuals who can offer extensive information. For this reason, senior experts were recruited in the interviewing process. Together, these approaches ensure that both the depth of knowledge and the ability to articulate complex ideas were considered in the selection process.

Incorporating cross-sectoral experts, as suggested by Chang, Pires, and Martinho [30], is particularly important for studying interdependencies in complex systems. This ensures a holistic understanding of the challenges and strategies involved in service management.

### 2.2.5 Conducting Interviews

The interview process was conducted in two rounds. The first round established a baseline understanding of service management practices in complex IT environments, while the second round focused on adaptive management strategies and evaluated specific approaches.

Both Hove and Anda [55] and Bogner, Littig, and Menz [23] emphasize the importance of a structured yet flexible interview environment to elicit high-quality data. Interviews were conducted via video calls or in person to ensure synchronous communication, allowing for real-time interaction and observation of non-verbal cues. Audio recording, with participants' consent, facilitated accurate transcription and analysis afterwards.

Creating a conducive interview environment was essential. Bogner, Littig, and Menz [23] and Saldaña [98] advocate for interviewers to adopt a non-judgmental, empathetic stance, using open-ended and non-leading questions to encourage detailed responses. Additionally, Mergel, Edelmann, and Haug [77] underscore the importance of clear communication and rapport-building during interviews. Suggesting a conclusion should invite further insights or nominations for additional participants.

To resolve uncertainties and enhance comprehension of important subjects, reflective questioning strategies were applied. Maintaining a research diary, as advised by Saldaña [98], assisted in capturing contextual nuances and personal reflections.

Post-interview workshops and the ability for continued contact from either the interviewer or interviewee post-interview, as recommended by Chang, Pires, and Martinho [30], were considered to validate initial findings and explore emergent interdependencies. This fostered a collaborative environment, encouraging experts to refine their inputs based on shared discussions.

### 2.2.6 Data Analysis

Thematic analysis was used for data interpretation, which includes transcription, coding, comparison, and validation. To guarantee a complete dataset, every interview was transcribed, and thematic codes were used to find important themes and reoccurring patterns. Example codes might include “Complexity Drivers,” “Adaptive Monitoring Strategies,” and “Regulatory Constraints.” These codes were then grouped into broader categories—such as “Automation and Resilience” or “Cultural and Organizational Dimensions”—to reveal patterns across all interviews [26].

Cooke and McDonald [36] advocate complementing thematic analysis with cognitive scaling techniques to reveal underlying patterns. Similarly, Li and Smidts [65] recommend utilizing weighted techniques to aggregate expert viewpoints, stressing the significance of sensitivity analysis in evaluating the robustness of findings. However, combining many of those approaches would be too detailed for this thesis. Iterative feedback loops during data synthesis, as proposed by Chang, Pires, and Martinho [30], helped refine insights and improve reliability. Clustering patterns in expert responses were also found using network

analysis. Strauss and Corbin [106] outline a three-stage coding process—open coding (identifying initial themes), axial coding (establishing relationships between themes), and selective coding (integrating themes into coherent categories). This multi-cycle coding approach ensures thorough analysis and helps derive well-structured conclusions.

The advanced qualitative analysis tool MAXQDA was used to manage and analyze the data. Maintaining transparency throughout the analysis is critical. Saldaña [98] recommends keeping detailed documentation of key decisions and reflections during analysis, ensuring that the research process remains well-documented and reproducible. By utilizing this method, the research intended to provide meaningful insights into service management strategies for complex IT environments, contributing significant knowledge to both academia and industry.

# Foundations of Complex Systems

## 3.1 Introduction to Complex Systems

Complex systems are fundamental phenomena found all around us, in natural, social, and technological domains. Their characteristic are an interplay of multiple interconnected components, where their interactions cannot be fully predicted by the analysis of an individual part in isolation, but rather through their emergent behavior [80]. Due to their unpredictability and dynamic nature, they advanced in various fields, ranging from ecology and economics to engineering and computer science. As the size of systems grows, their complexity grows in tandem. Understanding their behavior becomes essential to ensure stability, adaptability, and effective management [85].

The complexity theory and the study about complex systems provide a framework for how components interact, adapt, and self-organize in response to external and internal factors [111]. Emergent properties, feedback loops, and non-linear interactions are central to understanding these systems. These principles are reflected in various types of systems: Natural systems provide ecosystem stability and weather variation through these principles. Technological systems, exhibit these behaviors in the form of power grids, transportation networks, and increasingly IT systems [109]. IT systems in particular, over their distributed architecture, dynamic scaling, and high interconnectivity demonstrate these characteristics.

While the application and theory of complex systems has historically focused on natural and social systems, its relevance also shifted to technological domains. Especially IT systems now operate in highly dynamic environments where emergent behaviors, such as unexpected resource bottlenecks or cascading failures, can significantly impact the systems' reliability and performance. Therefore, studying complex systems offers important insights on how to deal with the difficulties of managing such environments [85, 111].

The fundamental ideas of complex systems are examined in this chapter, with a focus on important traits including emergence, non-linearity, and feedback loops. In order to contextualize the emphasis on complex IT systems in the following chapter, this chapter examines the various ways that complex systems theory is applied in the natural, social, and technological spheres. By drawing from seminal works such as Mitchell and Toroczkai [80], Tranquillo [111], and Thurner, Hanel, and Klimek [109], this chapter aims to establish a comprehensive understanding of complex systems as a conceptual and practical framework for analysing interconnected and adaptive environments.

## 3.2 Foundations of Complexity Theory

Complexity theory offers a framework for comprehending systems composed of numerous interacting components, where the behavior of the whole cannot be fully explained by examining individual parts. This section explores the fundamental ideas of complexity, focusing on emergent behaviors, self-organization, and the key characteristics of complex systems, followed by the models and methods used to study them.

### 3.2.1 Overview of Key Sources

Multiple frameworks and perspectives draw from complexity theory, each emphasizing different aspects. Newman [85] provides foundational tools and techniques in the form of a survey for studying them. His work explores concepts such as lattices, networks, dynamical systems, cellular automata, and scaling, offering a theoretical basis for understanding interconnectivity and emergent behavior. The relevance of these ideas is particularly important for analyzing large-scale systems, including IT networks, where interdependencies are found throughout.

In contrast, Tranquillo [111] conceptualizes the adoption of an application-oriented perspective, with an emphasis on emergence, feedback loops, and hierarchical organizations. This bridges practical applications with a theoretical foundation. This approach is particularly useful for adaptive systems, such as IT infrastructures. His concentration on real-world examples provides a clearer understanding of how complex systems act and evolve.

Thurner, Hanel, and Klimek [109] use a more mathematical and quantitative approach in which they delve into network science, Agent-Based Model (ABM)s, and evolutionary dynamics. With this a rigid framework for analyzing behavior and control mechanisms of complex systems with computational methods is provided. Developing models that mimic system behavior and forecast predictions in dynamic contexts is simplified using this viewpoint.

When combined, these perspectives offer a strong foundation for comprehending and evaluating complexity by fusing theoretical underpinnings, conceptual insights, and quantitative modeling.

### 3.2.2 Emergence and Self-Organization

The emergence phenomenon is one of the defining features of complexity, where interacting components show behaviors not directly observable or evident from properties of a single element of a system. It is a central concept of complexity theory, describing macro-level properties and how they emerge — such as the formation of weather patterns or flocking behaviors in birds — which arise from micro-interactions among individuals [80, 4]. For example, species interactions in ecosystems create dynamic yet stable settings, demonstrating the adaptability and resilience of emergent behavior [111].

Self-organization and emergence are often dependent characteristics, where systems structure themselves in a way where centralized control is not needed. Thurner, Hanel, and Klimek [109] describe self-organization as a process of local interactions between individual components, which in total lead to a global order. Examples of this phenomenon include the formation of traffic patterns, crystal growth, and the organization of distributed computing environments. The common denominator of these robust systems is the capability to adapt to change, yet their emergence makes it inherently unpredictable.

Since these concepts directly impact on system scalability and robustness, an understanding of emergence and self-organization is essential for managing large IT systems. Other examples can be found in distributed architectures, where individual components (e.g., servers) work together to maintain system stability under fluctuating loads. Similarly, self-organization is seen in peer-to-peer networks, which dynamically allocate resources based on demand.

### 3.2.3 Characteristics of Complex Systems

The following features of complex systems set them apart from simpler systems and are used to comprehend the emergence and evolution of complexity. Not every complex system necessarily exhibits all of them, but they illustrate key dynamics relevant for analysis.:

#### Non-Linearity

Non-linear interactions within complex systems mean that small changes in one component can lead to disproportionately large effects across the system [80, 4]. In chaos theory, the “butterfly effect” is a well-known example of this sensitivity to initial conditions. IT systems manifest non-linearity, as cascading failures, where a minor error in one subsystem can propagate, causing widespread disruption or outages [111].

#### Feedback Loops

System behavior can be regulated through feedback mechanisms, while positive feedback amplifies changes and can drive systems towards a new state (e.g., viral content spreading across social networks). Negative feedback does the opposite by counteracting deviations and stabilizing a system, such as load balancing in cloud computing [109]. Feedback loops

bring both adaptability and possible instability, requiring careful controls in dynamic systems.

### **Interconnectivity**

Components in complex systems are highly interconnected, creating dependencies that influence overall system behavior. Newman [85] highlights the significance of network structures in determining the robustness and efficiency of a system. For instance, distributed architectures in IT systems rely on interconnected nodes, where the failure of a single node can cascade through the network, highlighting the need for redundancy and fault tolerance.

### **Adaptability**

While adaptability is often present and enhances resilience, it is not a necessary condition of complexity. Complex systems constantly correct to adjustments in their environments. This is a property which enables the system to evolve and in the event of disruptions still maintain functionality. This is evident in biological systems such as immune responses, and in IT systems, such as cloud platforms and their auto-scaling mechanisms, where based on demand resources are dynamically allocated [111].

### **Scalability**

Scalability is frequently associated with complexity, as a characteristic of the ability to adjust capacity, resources or functionality in response to changing demand. In particular, in IT systems scalability is evident, cloud computing environments can dynamically allocate resources based on usage [85]. This ensures adaptability and that functionality remains prevalent and efficient under varying workloads, making it pivotal management mechanism of modern IT infrastructure. However, the architecture and planning of these systems to achieve a high degree of scalability requires careful considerations on the bottlenecks and interdependency within the system [109].

## **3.2.4 Modeling and Analysis of Complex Systems**

To study and understand complex systems, researchers apply various models and tools. These approaches provide insights into how components interact, how emergent behaviors originate, and how systems can be regulated or optimized.

### **Lattices and Networks**

Network theory and its components are a foundational model for understanding interconnectivity in complex systems. Nodes represent singular components, while the edges between them are the interactions. Newman [85] highlights the science of networks as a key tool for recognizing how connectivity influences robustness, efficiency, and

vulnerability. In IT, network models are used to assess data flow and detect bottlenecks. This information can be used to improve resource allocation in distributed systems.

### Cellular Automata and Discrete Dynamics

Cellular automata generate emergent behavior by simulating local interactions between discrete elements. These models are helpful for comprehending patterns and self-organization, including how information spreads in networks or how traffic congestion develops [80].

### Agent Based Models

ABMs simulate the actions and interactions of individual components (agents) to explore how system-level behaviors emerge. Thurner, Hanel, and Klimek [109] describe ABMs as a powerful tool for modeling adaptive systems, such as supply chains or IT infrastructure, where agents represent hardware or software modules.

### Scaling and Criticality

When it comes to managing IT systems, criticality refers to the tipping points where systems move from stable to unstable states, and scaling laws explain how system properties change with size. If not carefully managed, scaling under heavy loads can push the system towards failure [85].

### Information Theory and Computational Complexity

Information theory provides a framework for quantifying complexity; it describes the state of the system by measuring the information load [109]. Computational complexity examines the resources needed to solve problems inside a system, revealing insights into the limits of optimization and predictability.

Researchers can analyze complex systems at multiple scales by combining these models and tools, from big global behaviors to small local interactions. These methods are essential for modeling network performance, anticipating system faults, and creating flexible management plans in the field of IT.

## 3.3 Applications Across Domains

Complex systems are pervasive across natural, social, and technological domains, each characterized by unique interactions, emergent behaviors, and adaptability. Applying complexity theory to these domains provides insights into their underlying dynamics and offers strategies for managing their challenges effectively.

### 3.3.1 Natural Systems

Natural systems exemplify complexity through their intricate interactions and emergent behavior. For example, ecosystems are made up of interdependent species and environ-

mental elements that maintain a dynamic equilibrium [4]. Predator-prey dynamics, as described by Mitchell and Toroczka [80], highlight feedback loops that stabilize populations and ensure ecological balance. Nutrient cycling or forest succession demonstrates how local interactions lead to large-scale stability and adaptation [111]. Disruptions like damage to the habitat or species extinction, however, can have a domino effect and destabilize the system.

Weather systems also demonstrate complexity through non-linearity and sensitivity to initial conditions. Storms or droughts develop from intricate atmospheric interactions, often needing computational models to anticipate their progression [109]. Mirroring the more general ideas of complexity theory, these systems are prime examples of the interaction between interconnectivity and feedback loops, where minor adjustments can have major effects.

### 3.3.2 Social Systems

Social systems, including economic markets, urban environments, and organizational structures, demonstrate complexity. Supply-demand dynamics and speculative activity are two examples of feedback mechanisms that drive emergent behaviors, such as price fluctuations or market crashes. Overall, economic markets function as adaptive systems where buyer-seller interactions produce behaviors that frequently defy linear prediction [85].

Another example of social complexity can be found in urban systems, which are formed by interactions between infrastructure, people, and policies, resulting in highly interconnected networks [111]. For example, traffic congestion is caused by individual decisions that have an impact on the system as a whole, resulting in emergent patterns that call for adaptive management techniques.

### 3.3.3 Technological Systems

IT infrastructure embodies a technological system which provides complex networks due to their interdependencies and scalability requirements. Similarly, power grids and transportation networks rely on interconnectivity, where failures of a single node can propagate across the whole system or network, demonstrating cascading failures [109]. The goal of their system design is to maintain stability, yet the complexity makes it susceptible to emergent vulnerabilities. However, technological systems are never purely technical. They are better understood as socio-technical systems with their inseparable design and operation from human interaction.

IT systems pose distinct challenges as a subset of technological complexity. Their dependence on distributed architectures and rapid evolution calls for adaptive management strategies. For instance, cloud computing systems must dynamically allocate resources to meet fluctuating demand, a process influenced by feedback loops and non-linear interactions [85]. Similarly, cybersecurity threats frequently arise from component interconnectivity, necessitating systemic approaches to effectively mitigate risks.

#### 3.3.4 Conclusion

The application of complexity theory across these domains underscores its versatility and relevance. Complex systems in natural, social and technological contexts, can help researchers identify parallels in the design and management of their actors. From ecosystems to economic markets and IT infrastructures, complex systems share foundational principles that inform their behavior and management. Understanding these applications not only highlights the interdisciplinary nature of complexity theory but also allows for exploration into its specific implications for IT systems in subsequent chapters. The insights gained provide valuable lessons for addressing the challenges of technological complexity.

# Managing Complex Systems

## 4.1 Introduction

The management of complex systems has become an important discipline in modern organizational, technological, and industrial contexts. Unlike traditional systems, complex ones define their behavior through dynamic interdependencies, emergent behaviors, and non-linear interactions. With their inherently unpredictable features, conventional methods are not sufficient and innovative management methods are required. Interconnected infrastructures - such as power grids and transportation networks - have been increasingly critical, necessitating effective management of complexity [40, 67, 8]. Such systems need decentralized, adaptive techniques that can accommodate dynamic feedback loops with distributed control [67]. Furthermore, the role of human decision-making and cognitive limitations must be considered, as highlighted by Proctor and Zandt [90], to ensure that management strategies align with the inherent complexity of these systems.

The following sections delve into the principles of emergent management strategies, identify the key characteristics required for effective control, and the frameworks and models that enable adaptability and scalability in complex systems. By bridging theory and practical applications, this chapter aims to provide a comprehensive foundation for addressing the unique challenges of managing complex systems.

## 4.2 Principles of Management in Complex Systems

Effective management of complex systems requires principles that account for their non-linear interactions, emergent behaviors, and adaptability. This section explores three fundamental principles: emergent management strategies, decentralization and distributed control, and feedback-oriented control.

### 4.2.1 Emergent Management Strategies

Complex systems are characterized by emergent behaviors, which result from local interactions between constituents and frequently produce unexpected results. To fully utilize the adaptability that complex systems possess, it is imperative to manage these emergent behaviors. Moriarty [82] emphasizes pattern recognition and the opportune use of emergent behaviors. Employing these management techniques can result in new adaptive strategies for increased system resilience and efficiency.

Moriarty [82] further highlights that the philosophy from deterministic, top-down approaches must be changed to bottom-up processes, due to the change in the behavior of systems with emergence. Systems can effectively adapt to changing conditions by enabling local components to make decisions within a larger framework. This approach is especially pertinent in IT environments, where real-time interactions and distributed architectures necessitate flexible management strategies.

### 4.2.2 Decentralization and Distributed Control

Examining complex systems reveals that as interconnectivity increases, centralized control mechanisms struggle to maintain efficiency. Liu and Barabási [67] argue that a fundamental principle for managing such systems is by decentralization; this should increase robustness and reduce bottlenecks. Distributed control enables individual components to operate semi-independently while adhering to overarching system goals.

Additionally, human factors are important in distributed control. Clear communication, clearly defined responsibilities, and training to manage the complexity of interconnected systems are necessary for effective decision-making at the local level [90].

### 4.2.3 Feedback-Oriented Control

Feedback loops can be a management control apart from just being a feedback mechanism. They are necessary for sustaining stability and adaptation in complex systems. Åström et al. [8] emphasizes the two functions of feedback: negative feedback stabilizes the system by offsetting deviations, while positive feedback magnifies changes, spurring innovation and system evolution.

Boulangier [25] emphasizes the importance of formal methods for designing feedback mechanisms which in turn ensure reliability and precision. In practice, feedback-oriented control involves constant adjustments to system parameters, as well as continuous monitoring. For example, in IT systems, load balancers use real-time feedback to distribute workloads across servers, to prevent overloading and ensure seamless system management.

This principle emphasizes the need for tools and frameworks that can handle real-time data and successfully execute adaptive controls. By including feedback-oriented techniques, managers can cultivate systems that are both robust and sensitive to external stimuli.

## 4.3 Objectives and Properties of Managing Complex Systems

In this section, objectives and systemic properties of management that address the dynamic and unpredictable nature of complex systems are provided. These features guarantee that systems continue to operate effectively despite interruptions and shifting circumstances. They represent conditions to be achieved or challenges to be managed.

### 4.3.1 Resilience and Robustness

Resilience and robustness are not a method, but a desired outcome that are critical for managing disruptions in complex systems. Liu and Barabási [67] define resilience as a system maintaining functionality from a disturbance and its ability to recover it. Robustness refers to the system's capacity to withstand shocks without significant degradation. Åström et al. [8] highlights the significance of designing systems with inherent fault tolerance, such as failover mechanisms in IT infrastructures or redundant pathways in networks. These methods guarantee that the larger system continues to function even in the event of localized failures.

### 4.3.2 Adaptability and Flexibility

Complex systems can adjust to unanticipated difficulties and changing circumstances due to their adaptability and flexibility. Adaptive management techniques entail ongoing learning and iterative modifications [82, 8, 67]. It is further stated that flexibility in system design allows for rapid reconfiguration. By fostering adaptability, managers can ensure that systems endure unpredictable contexts [82, 8, 90].

### 4.3.3 Scalability of Management Approaches

Scalability refers to the capacity of a management approach to handle growth in system size and complexity. With the expansion of IT systems, their components grow increasingly interdependent. For example, hierarchical control structures or automated monitoring tools of scalable management strategies allow for efficient and performant strategies in distributed networks. As systems change, the capacity to scale and modify management procedures is essential to avoiding bottlenecks and guaranteeing smooth operations. Although scalability principles in complex systems are explored theoretically in debates like those by Boccara [22], practical applications of scalability concentrate on tools and architectures that support growth without compromising system functioning or stability.

### 4.3.4 Predictability vs. Uncertainty

Balancing predictability and uncertainty is a central challenge in managing complex systems. While certain system behaviors can be anticipated through modeling and simulation, emergent behaviors often defy prediction [67, 22, 40]. Boulanger [25], Åström

et al. [8], and Eisner [40] highlight the necessity of strong control systems that can handle uncertainty, like scenario planning or probabilistic models. This equilibrium guarantees that systems maintain their stability while maintaining the adaptability to deal with unanticipated changes. Managers can overcome complex obstacles and guarantee the long-term effectiveness and operation of their systems by balancing predictability with uncertainty.

## 4.4 Frameworks and Models for Managing Complex Systems

Complex systems must be managed using structured frameworks and models that offer instruments for monitoring, regulating, and optimizing their interconnected and dynamic nature. This section looks at the primary tactics that have been developed and refined for this goal.

### 4.4.1 Systems Thinking and Holistic Management

Holistic approaches and systems thinking focus on the different components, the connections and the relationships between them. Eisner [40] further advocates that complex systems should be viewed as holistic rather than a collection of isolated parts. Using this approach, managers can find leverage points where minor adjustments can result in major gains in system performance.

Machado and Lopes [69] expand this viewpoint by discussing symmetry in complex system architectures. The management and control of interconnected components is made easier by symmetry, which offers structural consistency. In IT systems, for example, symmetrical network topologies are able to streamline resource allocation and improve fault tolerance. The Viable System Model (VSM) developed by Beer [16] offers a cybernetic approach and complements systems thinking, to be more self-regulative and adaptable. VSM divides a whole system into recursive subsystems, with each having its own autonomous units for operations, coordination, controls, intelligence and governance. Each of these independent subsystems stays aligned with the larger system. The model focuses on managing interconnected and dynamic systems.

Building on these insights is Ashby's principle of requisite variety, which states that a control system must possess at least the same level of variety as the system it seeks to regulate [7]. Closely related is Beer's concept of black-boxing, highlighting that managers cannot fully grasp all internal dynamics of complex systems but must often rely on observable input–output relationships to regulate behavior [15]. Together, these concepts underline that holistic management requires both the development of governance mechanisms capable of matching systemic complexity and acceptance of systemic opacity.

### 4.4.2 Control Theory in Complex Systems

Control theory for complex systems establishes a mathematical basis for monitoring and optimizing dynamic behaviors. It is to differentiate from formal methods which focus on mathematical specification and correctness, since control theory primarily deals with feedback mechanisms and the dynamic behaviors of systems. Åström et al. [8] outlines their key principles and groups them into control theory, monitoring, stability and optimization techniques. Using these concepts, managers can create systems that sustain targeted performance levels in the face of internal and external disruptions.

In complex systems, this theory involves feedback loops which in turn should achieve stability. As an example, in the engineering field, these loops can be Proportional-Integral-Derivative (PID) controllers, which regulate variables such as temperature or pressure and consequently decide based on those measurements. Nigmatullin and Nougmanov [86] further integrates control theory to adaptive methods, which monitor system parameters in real-time and adapt to the measurements and changing conditions. Hollnagel, Woods, and Leveson [54] adopt a different approach and focus on the ability to anticipate, monitor, and adapt to disruptions; this ensures robustness and reliability.

### 4.4.3 Network-Based Control Strategies

Network-based control strategies identify important nodes and channels for efficient management by utilizing the interconnectedness of complex systems. Liu and Barabási [67] emphasize that knowledge of the network structure must be used to optimize system performance and prevent cascading failures.

For instance, in IT systems, identifying central nodes in a network can help managers prioritize resources and mitigate risks. Similarly, in order for a single node to not disrupt the entire system, redundancy and load-balancing strategies can be implemented. Network theory, the study of centrality, clustering, and resilience in networks, is valuable to have parameters for optimizations [12]. The Complex Adaptive Systems (CAS) Theory further reinforces the significance of emergent behavior and decentralized decision-making in the management of dynamic networks [53].

### 4.4.4 Formal Methods for Validation and Control

Formal methods are built up with a mathematical framework for verifying and validating behaviors of systems. Boulanger [25] emphasizes the role of formal methods in ensuring system reliability and stability by identifying and eliminating potential faults before they manifest. These techniques are particularly valuable in systems of critical infrastructure, such as avionics or medical devices, where errors potentially have life-threatening consequences.

For example, model checking and theorem proving allow managers to test various scenarios and configurations of a system under controlled conditions. This method guarantees that the system operates as intended in various operating scenarios. Organizations can improve

the predictability of complex systems and decrease uncertainty by incorporating formal methods into their management toolkit. In addition, decision-makers can use the Cynefin Framework [103] in conjunction with formal approaches to determine whether systems are functioning in chaotic or complex domains and to implement suitable validation strategies. In practice, however, the applicability of formal methods is often limited to well-defined subsystems rather than entire socio-technical infrastructures. As a result, formal approaches should be viewed as supplementary tools for certain situations rather than as a general management strategy.

## 4.5 Challenges in Managing Complex Systems

Considering complex systems are inherently unpredictable and dynamic, managing them remains a difficult task, even with the availability of sophisticated frameworks and models. The main difficulties managers encounter are examined in this section.

### 4.5.1 Balancing Adaptability and Stability

The balance between adaptability and stability is one of the core challenges of managing complex systems. Åström et al. [8] and Moriarty [82] highlight that while adaptability, excessive flexibility will reduce its stability. Stability can be understood in at least two ways. Static stability, where systems remain fixed and resist change, and dynamic stability, where systems maintain functionality precisely through continuous adjustment and feedback. In complex systems, stability is typically dynamic, as resilience emerges not from resisting change but from adapting to it [75]. The architecture of systems should be designed with strategies that allow a system to evolve and adjust without compromising the foundational integrity and stability. For instance, modular architectures that facilitate scalability and updates while maintaining essential functionalities are used in IT systems to achieve this balance.

### 4.5.2 Human Factors in Decision-Making

Human decision-making can pose challenges in managing complex systems, as cognitive limitations and biases can constrain effective decisions. Proctor and Zandt [90] therefore emphasize the design of systems which are decision-supporting and can enhance human capabilities rather than replace them with other decision-making systems. Examples of those include intuitive interfaces, real-time data, visualization and automated recommendations. This empowers assistance managers to make more informed decisions, especially in high-pressure situations. Furthermore, the influence of human error can be lessened via training programs that emphasize collaborative problem-solving and systems thinking.

### 4.5.3 Managing Emergent Risks and Systemic Failures

Complex systems, emergent risks and cascading failures are factors of highly interconnected parts. Moriarty [82] and Thomas, Prasad, and Mathew [108] note that identifying

and mitigating these risks requires proactive monitoring and predictive analytics. For instance, on machine learning or network firewalls, early warning systems exist, which can detect anomalies and predict potential disruptions before they escalate. Additionally, designing systems with redundancy and fault tolerant mechanisms in mind, can minimize the impact of localized failures and ensures that the overall system remains operational.

By addressing challenges such as balancing adaptability with stability, supporting human decision-making, and managing emergent risks, managers can navigate the complexities of modern systems more effectively. As systems become more complex, these initiatives are essential to ensure their sustainability and resilience.

## 4.6 Applications in Complex Systems

The management principles and frameworks discussed in previous sections are critically relevant in various complex systems. Some aspects of management are highlighted by multiple sources, particularly the need for adaptive and resilient management strategies. These applications span across domains, including ecological, organizational, and socioeconomic systems, where managing interdependencies and emergent behaviors is essential.

### 4.6.1 Relevance to Managing Complex Systems

The principles, such as adaptability, scalability, and feedback-oriented mechanisms of complex systems are relevant to a variety of domains. Eisner [40] and Moriarty [82] associate complex systems with the operation of dynamic environments, which in turn require managers to constantly adjust to shifting environments. For instance, resilience to environmental changes and maintaining biodiversity in ecological systems depend heavily on adaptability. Similarly, feedback loops are crucial in socioeconomic systems for maintaining market stability and implementing focused interventions to reduce systemic inequality.

In addition, feedback loops are also used in balancing resource allocation, such as in agricultural systems. Crop rotation and soil management practices rely on ecological understanding to provide soil fertility and productivity over time. It is further emphasized that the flexibility of resource management frameworks allows for adaptability to external influences, in this instance, climate variability or shifting needs by the consumers [82].

### 4.6.2 Real-World Examples of Adaptive Strategies in Complex Systems

If the focus shifts more towards adaptive strategies in complex systems and their real-world implementations, the versatility of these principles can be depicted. Moriarty [82] and Proctor and Zandt [90] argue in the context of disaster management systems that the continuity of services has to be provided during a crisis. Therefore, the attention on redundancy and fault tolerance has to be high. Localized resource redistribution is

frequently used in these tactics to reduce interruptions and efficiently assist impacted areas.

Machado and Lopes [69] elaborate on symmetric systems in urban planning, where symmetrical layouts improve traffic flow and reduce congestion. Urban spaces that plan emergent behaviors, such as fluctuating population densities, can ensure more sustainable and adaptable systems.

Lastly, network-based control strategies are another example of adaptive strategies in global supply chains. By dynamically redistributing resources and production capacity in response to variations in demand, these systems lower waste and improve resilience. Liu and Barabási [67] mention the importance of network structures and employ adaptive centrality-based strategies that prevent bottlenecks and failures which are cascading in the system.

The management of complex systems can handle difficulties in a variety of fields by combining these concepts and strategies. The application of frameworks on adaptivity ensures that complex systems stay responsive and robust. This is elaborated on the evolving challenges, whether in natural or socio-technical systems.

# Complex IT Systems: Foundations and Challenges

## 5.1 Introduction

Driven by increasing complexity, the financial sector has transformed rapidly in recent years. Its technologies, which once relied on centralized, monolithic IT architectures, have evolved towards distributed, cloud-based ecosystems, incorporating Artificial Intelligence (AI), blockchain, big data analytics, and open banking frameworks [60, 3, 91]. This transition has not only introduced new opportunities but also increased systemic risks and operational complexities.

The modern IT systems in which the financial industry operates are highly interconnected, with multiple actors — including banks, FinTech startups, regulatory bodies, and service providers — interacting in real-time. This mutual dependence leads to emergent behaviors, which can further lead to inefficiencies in ITSM or even system failures [114, 50]. Moreover, financial institutions must navigate evolving compliance requirements such as the General Data Protection Regulation (GDPR) [44], the Revised Payment Services Directive (PSD2) [43], Digital Operational Resilience Act (DORA), or Basel III [13], all of which impose stringent data governance and risk management frameworks [112, 71].

One of the key drivers of IT complexity in the financial sector is the adoption of cloud computing and microservice architectures. Unlike conventional on-premises IT infrastructures, these systems operate across distributed environments and necessitate advanced IT governance frameworks that support responsiveness with automated controls [10, 71]. Service-Oriented Architecture (SOA) can shift towards operational efficiency and facilitate scalability, but also introduce new challenges related to interoperability, cybersecurity, and IT service resilience [60].

Another major transformation in financial IT stems from the integration of AI and automation. AI-driven risk assessment, algorithmic trading, fraud detection, and customer relationship management are now core components of digital financial services [73, 112, 60]. Nonetheless, dependence on AI-driven decision-making raises concerns about transparency and the potential for cascading, bias-driven failures. This situation calls for adaptive ITSM frameworks to secure operational stability [3, 91, 60].

This chapter provides an in-depth analysis of the foundations of complex IT systems within the financial sector. It progresses from a historical evolution of financial IT to key characteristics of modern financial architectures, and finally to the primary components that contribute to complexity. Furthermore, it examines challenges associated with regulatory compliance, IT governance, security, and ITSM. By incorporating findings from recent academic research and industry best practices, this chapter seeks to create a framework for comprehending the complexities of contemporary financial IT systems and their ramifications for service management.

## 5.2 Evolution of IT Systems Toward Complexity

The evolution of the financial sector has undergone a profound technological transformation in the last few decades. There is a differentiation between traditional and modern IT systems. The following section outlines the historical trajectory that led to this complexity.

### 5.2.1 Historical Progression of Financial IT

Overall, there have been four distinct phases in the history of IT systems in the financial sector:

1. **Mainframe and Legacy Financial IT (1950s–1990s):** Early financial IT infrastructures relied on centralized mainframe architectures. These supported batch processing of transactions, policy underwriting, trade settlements, and financial reporting. These systems had minimal external connectivity and were highly structured and isolated [10, 96, 60].
2. **Client-Server and Core Financial Systems (1990s–2000s):** The shift to client-server architectures enabled more efficient processing in financial systems. While these systems improved accessibility, they remained monolithic and proprietary, with limited interoperability between financial institutions and regulatory entities [10, 60].
3. **Internet-Based Financial Services and Digital Transformation (2000s–2010s):** Advances in internet infrastructure and digital applications enabled instantaneous transactions as well as the automation of risk analysis and client interactions. However, as security and regulatory threats rose, more IT governance and compliance monitoring were required [112, 3, 60].

#### 4. Cloud Computing, AI-Driven Finance, and Digital-First Services (2010s–Present):

Modern financial IT infrastructures are cloud-native and AI-powered, enabling High-Frequency Trading (HFT), real-time risk modeling, algorithmic insurance pricing, and automated wealth management [60, 73, 10]. While FinTech, Insurance Technology (InsurTech), Regulatory Technology (RegTech), and the growth of digital financial services have all increased efficiency, they have also brought forth new difficulties with compliance and resilience.

As shown in Table 5.1, this progression reflects the increasing requirements in financial IT.

Time Period	Era	Key Characteristics	Technological Drivers
1950s–1990s	Mainframe IT	Centralized, batch processing	Mainframes, COBOL, relational databases
1990s–2000s	Client-Server IT	Monolithic, limited interoperability	Distributed databases, networking
2000s–2010s	Internet-Based Financial Services	Real-time transactions, digital trading, and risk management	Web services, encryption, API connectivity
2010s–Present	Cloud-Based and AI-Driven Financial IT	AI-powered automation, multi-cloud infrastructures	Cloud computing, big data, AI, RegTech, InsurTech

Table 5.1: Evolution of Financial IT Systems

#### 5.2.2 Future Trends in Financial IT Complexity

As financial institutions continue to evolve, the following trends will further shape IT complexity and have to be addressed:

- **Self-Adaptive IT Systems:** AI-driven observability tools will enable self-healing or at least self-monitoring, and autonomous security enforcement [60, 72, 111].
- **AI-Augmented Financial IT Governance:** AI-based RegTech solutions will assist in automated compliance and enhance fraud detection [73, 60].
- **Cloud-Native, Decentralized IT Architectures:** IT service delivery will be redefined by the ongoing adoption of serverless computing and API-first architectures, with an increasing shift toward blockchain-based financial services [10, 3, 60, 71].
- **Real-Time Risk Management and Predictive Analytics:** Machine learning models and AI, requiring significant computing power, will enable proactive risk

assessment in the business environment through cyberthreat mitigation and market anomaly detection [71, 60].

The future of financial IT will be defined by continuous innovation and evolution. As regulations increase and automation advances, institutions must move toward intelligent IT infrastructures capable of rapid response and significant processing power.

## 5.3 Defining Complex IT Systems

Modern financial IT systems are characterized by their tightly interwoven structures. While traditional systems were designed for static, self-contained operations, contemporary ones are inherently dynamic, exhibiting both interdependency and emergent adaptability [60, 3, 114]. This necessitates new governance approaches, risk mitigation strategies, and adaptive service management frameworks [17].

### 5.3.1 Key Characteristics of Complex IT Systems

Complex IT systems are defined by a high degree of interconnectivity for real-time operation and reliance on distributed architectures. In the financial sector, there are further demands including the support of massive transaction volumes, the compliance with stringent regulations, and overall high security standards across the entire infrastructure [91, 71]. Defining characteristics which are included in the financial IT systems are further listed in succession:

- **Interdependence and Non-Linearity:** Traditional IT systems operate on predictable, linear workflows, whereas modern financial IT environments exhibit non-linear dependencies, where small changes can have cascading effects across the entire system. Examples for this are third-party cloud services and interconnected financial APIs, as well as multiple interacting systems. This increases the risk of service outages propagating across the ecosystem due to cascading effects during an IT failure [50, 71].
- **Emergent behavior:** As financial IT systems become more integrated, new, often unpredictable behaviors emerge due to interactions between microservices, and real-time data. AI-powered HFT systems can amplify market fluctuations, leading to flash crashes and liquidity crises, ultimately creating an unpredictable market [3, 60, 50, 51].
- **High-Frequency Transactions and Automation:** The rise of HFT and automation, such as AI-driven credit scoring, or automated fraud detection has led to self-reinforcing feedback loops, increasing IT complexity and systemic risk as well as unpredictable decision-making. This can amplify false-positives and structural inefficiencies. Fraud detection and automated credit approvals are examples of systems that can lead to these effects [10, 60].

- **Scalability and Elasticity:** Unlike legacy financial IT, which was constrained by fixed, hardware-based infrastructures, modern financial IT must scale dynamically to accommodate fluctuating workloads and regulatory changes [3, 60, 5, 17].
- **Regulatory Compliance and Governance:** Financial IT systems must adhere to global regulatory frameworks such as GDPR [44], PSD2 [43], and Basel III [13], requiring real-time monitoring in combination with automated reporting, and cross-border data governance mechanisms [71, 114, 112].

Taken together, these are some of the characteristics that distinguish complex IT systems from their traditional counterparts, rendering their management increasingly challenging.

### 5.3.2 Comparison with Traditional IT Systems

The transformation from traditional IT to complex IT architectures in finance can be observed in multiple dimensions:

Aspect	Traditional IT Systems	Complex IT Systems
Architecture	Monolithic, centralized	Distributed, cloud-native, microservices
Scalability	Fixed infrastructure, limited scalability	Elastic, real-time scaling via cloud computing
Interconnectivity	Isolated, low external dependency	API-driven, interoperable, multi-cloud
Risk Management	Rule-based, human intervention	AI-driven, automated, predictive analytics
Regulatory Compliance	Manual audits, periodic reporting	Continuous monitoring, automated compliance
Service Availability	Limited redundancy, high downtime risk	High availability, fault tolerant architectures

Table 5.2: Comparison of Traditional vs. Complex Financial IT Systems

As seen in Table 5.2, traditional financial IT systems relied on monolithic centralized architectures, limiting scalability and interconnectivity. In contrast, modern financial IT systems are highly dynamic, API-driven, and cloud-based. This requires advanced governance frameworks and adaptive ITSM strategies that can cope with continuous change [60, 71].

### 5.3.3 Technological Components of Complex IT Systems

Multiple independent components form a modern financial IT system, which contribute to the overall system's complexity. In contrast to conventional monolithic structures, these systems incorporate cloud computing, big data analytics, AI, blockchain, and API-driven architectures to enable faster responses for scalable and efficient financial services [60,

114, 71, 10, 5, 68]. Each of these components possesses its own challenges in service management requiring tailored and adaptive solutions [73, 60].

### Infrastructure and Networking

Multi-cloud and hybrid architectures have evolved from centralized data centers and on-premises solutions in the financial IT infrastructure. This enables better distributed computing with redundancy and scalability. The key aspects of modern financial IT infrastructure include:

- **Cloud Computing and Virtualized Environments:** Financial institutions are progressively utilizing multi-cloud and hybrid cloud architectures to attain elasticity, which work cost-efficiently and are highly available, while addressing interoperability and security threats [5, 60, 10, 71].
- **API-Driven Financial Ecosystems:** The rise of open finance services with FinTech integration and real-time financial provisioning is powered by secure API gateways that enable seamless data exchange and interoperability between financial institutions and third-party service providers [60, 10, 91, 3, 112].
- **High-Speed Financial Transactions and Network Infrastructure:** Low-latency networks (5G, fiber optics, Software-Defined Wide Area Network (SD-WAN)) support real-time operations, but also increase demands for IT performance monitoring and cybersecurity measures [60, 10, 73, 3].
- **IT Orchestration and Automated Service Management:** The transition to cloud-native IT demands a rethinking of operational models, in which automated service provisioning supports scaling and continuous monitoring. This guarantees resilience and reliability for the system and provides an efficient incident response process that ensures regulatory compliance [60, 10, 91, 3].

These developments improve system resilience and efficiency, but they also bring new risks, especially in managing regulatory exposure and safeguarding multi-cloud systems [112, 71].

### Data Management and Processing

The financial sector is exceptionally data-driven, necessitating scalable and effective data management frameworks. Key aspects of financial data processing include:

- **Big Data Analytics and AI-Powered Decision-Making:** AI and machine learning models have multiple uses e.g. credit scoring, algorithmic trading, fraud detection, and customer behavior analysis. This requires real-time processing and automated governance [60, 73].

- **Data Warehousing and Real-Time Processing:** Financial institutions leverage distributed storage architectures (Hadoop Distributed File System (HDFS), Not only SQL (NoSQL), and columnar databases) to efficiently handle large-scale structured and unstructured financial data [68, 60, 114, 10].
- **Regulatory Data Compliance and Governance:** Financial IT systems must ensure data privacy and the Confidentiality, Integrity, Availability (CIA) triad to comply with GDPR [44], PSD2 [43], Basel III [13], and other regulatory frameworks [71, 114, 112].
- **Data Integration and Interoperability Challenges:** As dependence increasingly spans across multi-cloud systems and external interfaces or open financial ecosystems, standardized, interoperable data exchange becomes essential to ensure continuity in transactions and reporting [60, 50, 3].

These advancements in data-driven decision-making improve efficiency but increase dependency on complex data governance models, requiring automated risk assessment frameworks for management purposes [71, 60, 50].

### Security and Risk Management

Cybersecurity and operational risk management become critical concerns as complexity grows in financial IT systems. Key security and risk challenges include:

- **Zero-Trust Security Architectures:** Financial institutions implement multi-layered authentication and Identity and Access Management (IAM) to mitigate security risks [60, 71, 73].
- **Regulatory Compliance and IT Audits:** Global compliance rules must be followed by financial IT, which calls for automated compliance monitoring systems and audit trails for reporting [71, 112, 114, 60].
- **Threat Intelligence and Incident Response:** AI-based cyberthreat detection allows for prediction and real-time reactions to improve IT resilience and utilize Security Operations Center (SOC) with a Security Information and Event Management (SIEM) [71, 60].
- **Operational Resilience in HFT Systems:** Strong cybersecurity and fault tolerance are essential for real-time trading systems, which call for self-healing IT infrastructures that can identify and address problems by autonomously detecting and mitigating failures [60, 3].

As cyberthreats evolve, organizations must implement adaptable security frameworks with proactive detection and intelligent response capabilities [71, 60].

## Automation and Orchestration

Automation is a key enabler of operational efficiency and service resilience amid the growing complexity of financial ITSM. Some critical aspects of IT automation include:

- **AI-Based ITSM (Artificial Intelligence for IT Operations (AIOps)):** AI-driven service orchestration enhances real-time incident response in ITSM environments while optimizing cloud resources [97].
- **Predictive Maintenance and Self-Healing IT Systems:** Financial organizations can deploy self-correcting infrastructures through automated IT governance solutions that proactively identify issues [60, 112].
- **Automated Compliance and RegTech Integration:** AI-powered RegTech solutions streamline compliance and audit reporting, integrating features such as fraud detection [73, 60, 112].
- **AI-Driven Trading and Market Surveillance:** Machine learning models optimize HFT strategies by enabling AI-driven decision trading systems and increased market surveillance through automated data analysis [10, 60, 3].

Automation and AI governance will be essential to preserving stability, security, and support in compliance as financial IT develops [60].

### 5.3.4 Conclusion

As financial IT systems have evolved into highly complex and distributed environments, they have also introduced new challenges. The integration of cloud computing, AI, big data, and blockchain has enhanced efficiency and scalability, while also introducing new risks and management demands in security and compliance [60, 3, 71, 112]. Currently, proactive risk assessment techniques using AI-driven automation and flexible governance frameworks are necessary for efficient ITSM.

## 5.4 Complexity in ITSM

The increasing complexity of financial IT systems has introduced technologies such as cloud computing and AI, which pose significant challenges for ITSM. Traditional frameworks were originally designed for structured, centralized environments, but need to keep evolving with the evolution of the infrastructure and services. Information Technology Infrastructure Library (ITIL) [9], Control Objectives for Information and Related Technologies (COBIT) [58], and ISO/IEC 20000 [57] are examples of frameworks which evolved with the landscape and remain relevant [60, 10].

As financial systems transition from traditional to complex architectures, three major implications for ITSM become evident. The shift from manual to automated service

management practices, stronger integration of risk-based governance, and a focus on resilience and Business Continuity Management (BCM).

With the move towards cloud and decentralized IT architecture, ITSM is therefore required to adapt to dynamic environments, which require real-time service provisioning and adaptive workloads [10, 3, 71]. The structural characteristics outlined in this chapter translate directly into operational challenges for IT service management. The following section dives into the impacts of ITSM in financial IT complexity. This highlights the challenges of traditional approaches, adaptive ITSM strategies, and the role of AI and automation in ensuring faster response times and better decision-making.

### 5.4.1 ITIL and ITSM Frameworks in Financial IT

Traditionally, ITSM is organized around process-oriented frameworks such as:

- **ITIL:** Is a framework which provides best practices for ITSM. It focuses on structured incident management, change control, and problem resolution, ensuring service reliability [101, 71, 9].
- **COBIT:** Is an IT governance framework that helps with implementation and monitoring. COBIT provides IT governance and compliance models for risk management and regulatory alignment [101, 71, 58].
- **ISO/IEC 20000:** Defines a global ITSM standard to ensure consistency and Service-Level Agreement (SLA) compliance [101, 57].

While these frameworks offer structured and standardized methods for ITSM, they frequently struggle to adapt to the dynamic characteristics of cloud-native or AI-driven systems with diverse microservices. This necessitates service management practices that are more flexible and modular with fast responses [101, 60].

### 5.4.2 Challenges of Traditional ITSM in Complex Financial IT Environments

The following are challenges and limitations faced by the ITSM frameworks in complex financial IT systems:

1. **Rigid Change Management Processes:** ITSM frameworks emphasize manual change approval workflows over multiple committees, which are too slow for agile development and service changes [71].
2. **Lack of Real-Time Incident Response:** Traditional incident management relies on human intervention and gathering of multiple stakeholders, whereas modern financial IT requires real-time anomaly detection and automated mitigation, often supported by AI [84].

3. **Service Resilience in Cloud-Native IT:** Capabilities like automated fault tolerance and self-healing architectures help with service resilience. Predictive IT monitoring is necessary to detect problems in cloud-based financial services. However, traditional ITSM frameworks were not originally designed to meet these requirements and offer only limited guidance in implementing such dynamic and intelligent service models, especially given the lack of transparency in cloud environments [60].
4. **Regulatory and Compliance Constraints:** Financial regulations such as GDPR [44], PSD2 [43], and Basel III [13] demand continuous monitoring, automated compliance reporting, and data governance, which exceed the capabilities of static ITSM models and calls for stricter regulations [96, 60].
5. **Scalability and Multi-Tenant IT Management:** Financial institutions operate across multi-cloud environments with diverse stakeholders and interconnections between tenants. This requires flexible governance structures that require service reliability and cross-cloud service integration [60].

Due to these restrictions, ITSM must undergo a fundamental change that keeps advancing toward self-adaptive and risk-based IT service models.

### 5.4.3 Adaptive ITSM Strategies for Complex IT Systems

Due to some limitations in traditional ITSM, financial institutions are shifting towards more adaptive strategies. Blending automation with adaptability and aligning more closely with risk-based decision-making:

- **AI-Based IT Service Orchestration:** AI-powered tools enhance incident response and enable faster handling. They can also help with Root Cause Analysis (RCA) and IT governance [61].
- **Proactive Risk Management and Anomaly Detection:** AI-driven analytics enable predictive service monitoring; this reduces downtime and IT disruptions [74].
- **Cloud-Native ITSM and Development and Operations (DevOps) Integration:** Modern financial IT requires automated service provisioning through Infrastructure as Code (IaC), and Development, Security, and Operations (DevSecOps)-driven IT governance established by Continuous Integration / Continuous Delivery (CI/CD) pipelines [107].
- **RegTech for Automated Compliance:** RegTech solutions powered by AI simplify the processes of regulatory reporting and enforcing compliance [3, 60].

- **Resilient, Self-Healing IT Systems:** AI-driven self-healing mechanisms in the form of Security Orchestration, Automation, and Response (SOAR) enable autonomous incident resolution with service restoration, and automated rollback of failed changes [95].

These approaches allow financial institutions to modernize their ITSM strategies by addressing challenges that go beyond the most well-known ITSM frameworks.

#### 5.4.4 Automation and AI-Driven ITSM

As previously mentioned, the integration of automation through machine learning or predictive analytics is revolutionizing ITSM by enabling:

- **Automated Incident Management and Response:** AI models analyze historical IT incidents and trigger automated remediation workflows based on predefined procedures [39].
- **Predictive Maintenance and Service Optimization:** AI-powered monitoring systems anticipate IT failures and improve infrastructure performance by addressing issues before they occur [39, 18].
- **Intelligent Change Management and DevSecOps:** AI assists in automated impact assessment, calculates risk scores, and provides continuous compliance validation for IT changes [39, 48].
- **Digital Twins for IT Service Simulation:** Digital twins allow institutions to simulate service disruptions, enabling a resilience strategy which optimizes IT service delivery based on actual scenarios [39, 76].
- **Real-Time Fraud Detection and Security Analytics:** Financial transactions are regularly examined by AI-based security systems for anomalies in the behavior. This detects cyberthreats and fraudulent activities [18, 112].

In complex financial IT settings, AI-driven ITSM guarantees increased efficiency and robustness while lowering operational risk and service interruptions.

#### 5.4.5 The Future of ITSM in Finance

The future of ITSM models can already be predicted to some extent. As financial IT complexity continues to grow, the focus shifts to:

- **Fully Autonomous IT Operations (AIOps):** AI will manage IT services autonomously, reducing manual intervention and improving service efficiency. Agent-based AI models can leverage complex tasks with an easy interface for human interactions [1].

- **Decentralized and Blockchain-Based IT Governance:** Smart contracts will enable automated SLA enforcement. As a result, trustless service auditing and real-time compliance monitoring become possible [102].
- **AI-Enhanced IT Security and Cyber Resilience:** AI-driven threat intelligence will provide adaptive security models, reducing IT vulnerabilities and cyber risks, while also bringing new threat actors, which also have to be managed [59, 112].
- **Digital Assistants and AI-Powered ITSM Chatbots:** Chatbots powered by AI will improve knowledge management and communication within IT support and service desk automation [29].
- **Continuous Compliance and Regulatory Evolution:** ITSM must adapt to dynamic regulatory changes, requiring real-time AI-powered audit trails, compliance dashboards, and automated reporting. This enhances monitoring and provides data for future decisions [38].

#### 5.4.6 Conclusion

Complex modern financial IT ecosystems demand the evolution and redefinition of certain parts of ITSM frameworks. Traditional ITSM models such as ITIL [9], COBIT [58], and ISO/IEC 20000 [57] are already evolving to support AI-driven automation in cloud-native infrastructures, and can even extend to providing predictive service orchestration [60, 61, 39]. To guarantee service resilience while maintaining regulatory compliance and operational efficiency in an increasingly complex financial sector, institutions must adopt ITSM methods that are adaptable and automated.

## 5.5 Challenges in Managing Complex IT Systems

While challenges of managing complex IT systems have been mentioned throughout this chapter, this section expands on this further. From increasingly interconnected and cloud-native systems to their management, significant challenges arise from different drivers [60, 71, 61, 39]. From monolithic architectures to distributed, microservices-based ecosystems, their associated risk, unpredictability, and emergent behavior make traditional management approaches inadequate [112, 50].

This section explores the key challenges in managing complex IT systems, focusing on systemic risk, security vulnerabilities, compliance constraints, IT governance issues, and the unpredictability of emergent behaviors.

### 5.5.1 Systemic Risk in Financial IT Ecosystems

Systemic risks refer to the potential for localized failures to propagate across an interconnected IT environment with cascading effects. This can result in widespread disruptions, and in complex financial IT systems, this systemic risk arises due to:

- **Interconnected IT Dependencies:** As they depend on cloud computing with multiple connected interfaces and third-party service providers, financial institutions are susceptible to supply chain interruptions and cascading failures [96, 60].
- **Algorithmic Decision Loops:** AI-powered trading and credit risk assessment algorithms have the potential to introduce self-reinforcing feedback loops, which can amplify market volatility and IT system instability [2].
- **HFT Failures:** The automation of real-time trading and liquidity management introduces latency-sensitive risks. Minor network disruptions can trigger large-scale financial instability due to the inability to respond to the financial market [87, 60].
- **Data Breach and Information Leaks:** When security flaws in one institution jeopardize interbank networks and result in significant data breaches, systemic risk increases [60].

As financial IT environments become more automated and interconnected, it becomes harder to mitigate systemic risks. Therefore, real-time monitoring with predictive analytical capabilities and dynamic risk assessment models are required [60].

### 5.5.2 Security and Cyberthreats in Complex IT Environments

The increasing reliance on technology and complex infrastructures has introduced new cybersecurity risks that financial institutions must address to stay resilient:

- **Expanded Attack Surface:** As financial institutions adopt multi-cloud architectures and open APIs, they expose themselves to new attack vectors, such as API-based exploits, and cloud misconfigurations. In these cases, institutions are not in full control of these environments [35].
- **AI-Powered Cyberthreats:** Attackers are using AI and machine learning to create phishing schemes, automate cyberattacks, and circumvent conventional security measures. Moreover, the use of AI also introduces new attack vectors on its own [56].
- **Regulatory Challenges in Cybersecurity:** Financial institutions must comply with GDPR [44], PSD2 [43], Basel III [13], DORA [46], and Markets in Financial Instruments Directive II (MiFID II) [42], all of which impose stringent security and data protection requirements to enhance resilience and protect assets [38].
- **Zero-Day Vulnerabilities in FinTech Solutions:** FinTech-driven applications raise the possibility of undiscovered security flaws by introducing new code bases and decentralized financial models, compounded by newly introduced third-party dependencies [79].

In order to address these risks, mitigation actions must be implemented. Financial institutions have to implement security concepts such as zero-trust security architectures. Additionally, they are supported by AI-driven anomaly detection and continuous compliance enforcement tools.

### 5.5.3 Regulatory and Compliance Challenges

The evolving regulatory landscape requires financial institutions to implement more compliance mechanisms [60, 38, 63]. Major compliance challenges include:

- **Cross-Border Data Regulations:** Financial institutions operating in multiple jurisdictions must comply with different national and international regulations at the same time, including GDPR (EU) [44], California Consumer Privacy Act (CCPA) (US) [27], and Open Banking (UK) [34]. The regulation of the jurisdiction of the user data has to be considered, as well as the data processor [60].
- **RegTech Adoption:** Institutions must integrate AI-powered RegTech solutions. This automates regulatory compliance and provides audit trails [3, 60].
- **Continuous Monitoring Requirements:** Financial organizations must use AI-driven monitoring and dynamic compliance models as regulatory authorities enforce real-time compliance [38].
- **Auditability of AI-Driven Decisions:** Financial regulators demand transparent decision-making models including those driven by AI, yet black-box AI models introduce interpretability challenges [63].

Regulatory frameworks are continuously evolving, requiring IT leaders to implement and adapt to compliance models and automated governance tools.

### 5.5.4 IT Governance and Operational Challenges

New approaches to IT governance and operational resilience are required for complex financial IT systems. Key governance challenges include:

- **Cloud Service Provider (CSP) Dependencies:** Financial institutions increasingly rely on AWS, Microsoft Azure, and Google Cloud, but governance challenges arise due to shared responsibility models and potential CSP outages [71, 10].
- **IT Service Continuity and Disaster Recovery (DR):** For automated incident response and real-time failover, traditional DR models need to be adapted. Strategies include the implementation of geo-redundancy and continuity plans [60].
- **Operational Complexity of Microservices-Based IT:** Unlike monolithic architectures, microservices introduce service sprawl and dependency failures, making operational resilience more difficult and requiring lower latency [3].

- **Emergent behaviors in Automated Financial Systems:** Algorithmic trading and AI-driven market prediction can all have unanticipated consequences that call for immediate human supervision and emergency response plans with suitable risk modeling [73].

To address these governance challenges, financial institutions should integrate AI-driven ITSM, predictive analytics, cloud governance models, BCM or DR plans [60].

### 5.5.5 Emergent IT Failures and Self-Reinforcing Risks

Complex IT systems exhibit emergent behaviors resulting from unpredictable interactions between interacting components. This unpredictability can lead to failures and systemic disruptions; therefore, key challenges emerge [60, 51]:

- **Cascading Failures in Distributed Systems:** Microservices-based architectures introduce dependency chains. The failure of a single service can trigger network-wide outages. After an outage, the DR also has to follow the dependency chain [64].
- **Automated Decision-Making and Market Volatility:** AI-driven financial markets rely on automated trading algorithms, but self-reinforcing behaviors can create flash crashes and liquidity crises, which require monitoring [39, 2].
- **Cloud-Native Configuration Drift:** Configuration drift occurs when cloud applications are continuously deployed, causing security settings and rules to become inconsistent across various environments [107].
- **AI Bias and Unintended Consequences:** Financial decision-making models can exhibit biases, leading to unintended consequences in credit approvals and fraud detection. These biases can also discriminate against certain user groups and lead to regulatory violations [92].

Understanding these emergent risks requires continuous monitoring of AI-driven decisions; this can be established through a proactive ITSM strategy.

### 5.5.6 Conclusion

Managing complex IT systems in financial institutions requires new strategies. A holistic and multi-layered approach should integrate AI-driven security, adaptive risk governance, and cloud-native resilience [39, 60, 107]. Financial institutions should use automated regulatory compliance and real-time IT service monitoring as IT complexity increases, in order to reduce systemic risk and guarantee regulatory alignment. Lastly, threat intelligence and response capabilities are critical for maintaining reliable service resilience [38, 56].

## 5.6 Conclusion

The evolution of financial IT systems has led to unprecedented levels of interconnectivity and complexity. Key drivers in these ecosystems include the integration of cloud computing, AI-driven decision-making, microservices, and real-time data processing [60, 3, 91, 10]. To manage these developments, adaptive IT governance, predictive risk management, and automated service orchestration are essential for maintaining operational resilience and regulatory compliance [71, 112, 60].

The distinguishing features of complex IT systems have been described in this chapter, along with their historical development and the main technological forces that have contributed to their growing complexity [96, 114, 3]. Financial institutions today must navigate emerging sources of systemic risks, cybersecurity threats, compliance constraints, and IT governance challenges. This requires a shift towards more fast-paced strategies, including AI-driven service management and proactive IT resilience [39, 60, 38].

### 5.6.1 Key Findings

The main findings of this chapter can be summarized as follows:

- **Complex IT Systems Are Highly Interconnected:** Cloud computing, open financial APIs, and multi-tiered service architectures are all essential components of financial IT infrastructures, which increase service dependencies, regulatory issues, and systemic dangers [60, 10, 71].
- **AI and Automation Are Reshaping IT Governance:** Traditional ITSM frameworks such as ITIL [9], COBIT [58], and ISO/IEC 20000 [57] are evolving to real-time, AI-driven decision-making. This evolution enables IT service orchestration and predictive IT maintenance, complemented by additional strategies [39, 60, 73].
- **Cybersecurity and Compliance Are Key Challenges:** Financial institutions face growing threats from AI-powered cyberattacks, regulatory scrutiny, and multi-jurisdictional compliance mandates, necessitating zero-trust security architectures and AI-driven compliance automation [38, 60, 71].
- **Emergent Risks Require Predictive Analytics:** High-frequency transaction processing, automated trading, and AI-based financial models introduce self-reinforcing risks due to their unpredictability, necessitating automated IT monitoring, real-time anomaly detection, and predictive risk assessment [50, 51, 60].
- **Financial IT Must Adopt Adaptive ITSM Strategies:** To address operational complexity, regulatory demands, and service resilience requirements, financial ITSM must constantly adapt. This is achieved through AI-driven automation, predictive analytics, and cloud-native governance frameworks [60, 61, 3].

### 5.6.2 Implications for ITSM

As financial IT complexity grows, traditional ITSM approaches must be adjusted to accommodate dynamic environments, faster financial transactions, and emerging risks [60, 71]. The implications of these findings for ITSM include:

- **The Shift Toward AIOps:** Financial institutions need to deploy AI-driven service orchestration with automated incident response capabilities and self-healing IT infrastructures [97, 39, 60].
- **Regulatory-Driven IT Automation:** AI-powered RegTech solutions will play a crucial role in real-time compliance enforcement, including automated reporting and fraud detection features [3, 60, 38].
- **Cybersecurity Must Be Adaptive and Intelligence-Driven:** Financial IT needs an adaptable, AI-enhanced threat intelligence framework since traditional perimeter-based protection is insufficient [35].
- **Cloud Governance Must Balance Innovation and Risk:** The development of multi-cloud resilience strategies ensures fault tolerance and secure, API-driven integrations across heterogeneous systems [3, 60, 63].

# Service Management Strategies for Complex IT Systems in the Financial Sector

## 6.1 Introduction

While IT systems have grown increasingly complex, this has been further amplified by the service management demands in the financial sector. A modern financial institution no longer operates as a singular monolithic and isolated platform but is embedded in a highly interconnected and dynamic financial ecosystem. Multiple actors operate in the financial ecosystem, financial institutions, markets, regulatory bodies, consumers, and technological providers are some of them, each with its own characteristics and requirements [60, 96, 19]. These ecosystems not only exhibit different actors but also traits when observed from the perspective of complex IT systems: multiple interacting components, decentralized control structures, feedback loops, and emergent behaviors which do not obey linear cause-effect reasoning [105, 66, 81].

Technological and institutional transformation both drive the rise of complexity in financial IT systems. Dependencies are driven by the integration of multiple complex technologies, such as the cloud and automation; these transformations accelerate the pace of change. Concurrently, financial institutions have to navigate through regulatory mandates and customer requests, which contribute to the complexity of the organization's systems. Also, cyber resilience is another driving demand [71, 3, 91]. These circumstances call into question conventional beliefs regarding service management and system boundaries.

These dynamics can be understood through the valuable lens of complexity theory. It underscores the shortcomings of deterministic planning and hierarchical control, advocating for governance strategies that are adaptive and system-aware. Service managers have

to translate this into the management of uncertainty and anticipate emergent risks. But overall design resilient practices to align with this type of characteristics in a system [81, 66, 111].

Modern service management should address the structural and behavioral complexity of the socio-technical systems it supports, rather than concentrating solely on technical performance. In this sense, frameworks such as ITIL, which have already been relevant for ITSM in traditional systems, need to be applied with greater flexibility to the evolving conditions. As mentioned by MacLean and Titah [70], these frameworks must be adapted to fit scale, speed, and ambiguity inherent in complex financial systems. The increase in complexity correlates with reduced predictability and transparency, which in turn escalates the operational burden on service managers and demands new processes [19, 66].

This chapter explores approaches used to manage services in complex IT environments within the financial sector, from strategic to operational. Specifically, how institutions define responsibility boundaries, align ITSM methods with business and regulatory requirements, and implement monitoring and automation will be explored. Through a synthesis of academic literature, industry frameworks, and selected empirical findings, these elements will be evaluated. The chapter builds upon the prior theoretical discussion of complexity by operationalizing its implications for service delivery and operational control.

While most of the literature concentrates on service management in relatively stable or modular systems, here the focus is on high-complexity environments. These environments are often defined by multiple different complexity drivers [60, 96, 10]. This perspective lays the groundwork for the subsequent empirical analysis, which investigates how financial institutions use and adapt to service management strategies in real complex business contexts.

## 6.2 Impact of Increasing IT Complexity on Service Management Practices

Digital ecosystems, regulatory growth, competitive FinTech innovation, and multi-layered service delivery models are some of the convergent transformation layers that have contributed to the acceleration of IT complexity in financial institutions rather than just technological innovation. Aspects of this multi-dimensional growth in system complexity directly affect how service management must be structured [60, 3, 96, 20].

A contributor to the increase of this complexity is architectural heterogeneity. The existence of varied system components within an IT landscape, each with its own technological underpinnings, is referred to as architectural heterogeneity. Financial service landscapes are now composed of modularized systems — core banking engines, customer interfaces, regulatory reporting layers, and third-party integrations — often governed by separate lifecycle and ownership models [10]. Apart from the technical

diversity, these systems also often evolve at different cadences, creating complications in aligning continuity across the service stack. Unlike monolithic systems, modern financial IT do not fail predictably, but rather exhibits cascading effects and opaque failure propagation due to the high interdependency [81, 64].

From a complexity theoretical perspective, these phenomena further reflect characteristics of CAS. Composed of different in- and interdependent components that interact dynamically. Linear controls fail to address the behaviors produced by the individual parts in isolation and cannot guarantee the stability of the system [66, 81, 111]. For service management, issues such as incident propagation or regulatory misalignment can result from non-linear interactions between systems, policies, and teams.

Moreover, institutional complexity is amplified by dual transformation pressures: innovation and compliance. The need to integrate real-time payment schemes, such as Society for Worldwide Interbank Financial Telecommunication (SWIFT), the global messaging network that enables secure and standardized financial transactions. In addition to this system, open banking APIs, and cross-border services create a rapid pace for system change and inter-organizational coupling [91, 60]. Operational standards are raised simultaneously by changing regulatory requirements, such as DORA [46] and MiFID II [42], which require that every process remain auditable and resilient [112, 71].

Both the strategic and operational levels of service management procedures are burdened by different dynamics. Strategically, ITSM must balance agility and control; change must be enacted quickly while adhering to governance frameworks that reduce systemic risk and guarantee regulatory compliance [19]. Operationally, incident resolution with identification of the root cause, and monitoring processes must scale across fragmented and federated architectures [70, 84]. This highlights the challenges of operational fragility, where small perturbations in one part of the system may escalate through the service layers.

The correlation between financial systems complexity and service fragility is consistent with more general conclusions drawn from complex systems theory. As Lindgren [66] and others have argued, the system's entropy increases with scale and the degree of interconnection, making continuous management efforts important to ensure stability. Financial institutions, especially those using hybrid cloud and global markets, must therefore experience a service management paradigm, which supports proactive intervention through automation and observability platforms.

Modern ITSM techniques must deal with feedback loops, multi-agent interactions, and uncertainty as operational constants, in contrast to classical ITSM, which frequently assumes system modularity and linear causation. According to complexity theory, systems with changing structures and behaviors are better managed by adaptive responses rather than rigid processes [81, 30, 14, 31]. The focus shifted from merely maintaining basic functionality to dynamically allocating attention and resources to ensure customer and regulatory demands under variable conditions.

## 6.3 Demarcation of Service Management Responsibilities in Complex Environments

### 6.3.1 Organizational vs. System-Level Responsibilities

As financial IT infrastructures become more complex, the delineation of responsibilities between organizational units and system-level functions becomes a more prominent component of effective service management. Traditional IT organizations rely on centralized service management structures, where modern ITSM units are responsible for more specialized tasks. However, this traditional model proves to be inefficient in environments of distributed systems with microservices and cross-functional teams [81, 104, 10, 31].

Other models, like the decentralized ownership models inspired by DevOps, Site Reliability Engineering (SRE), and service-based accountability promote direct embedment of service management practices into teams responsible for the development and operation. In this, individual service teams are accountable for the delivery of functional features, as well as the ongoing operation and overall performance of their systems. This could include KPIs such as uptime or incident response [72, 21, 24]. The focus shifted towards the mentality of ‘you build it, you run it,’ particularly within institutions whose models emphasize product-centricity and agility.

Due to the distributed nature of the complex systems, the control of them also should be distributed rather than centralized. Top-down orchestration is not sufficient in environments with significant interconnection and non-linear behavior. Instead, modular governance structures are advantageous for complex systems because they allow local actors, like service teams, to manage subsystems with some degree of autonomy while still staying in line with higher-order constraints [40, 81, 66].

With this change from local ownership to distributed responsibility, it brings another level of organizational complexity due to newly introduced governance challenges. Without a clear coordination structure, service management tasks may become fragmented or inefficiently redundant [19, 70]. Moreover, in highly regulated sectors such as finance, the demarcation of responsibilities must accommodate external constraints, Segregation of Duties (SoD), compliance monitoring, and audit requirements [71].

Effective governance in such environments has been underscored by complex system engineering research, it requires meta-level structures that coordinate the behavior of subsystems without centralizing the decision-making [81, 89]. This translates into hybrid governance models in service management, that balance a standardized oversight with autonomy. Some common strategies include service governance boards, federated Change Advisory Board (CAB)s, and unified service catalogs to align with decentralized operations overlooking enterprise-wide initiatives [72].

Ultimately, the demarcation of responsibilities in complex IT environments is dynamic and evolves in tandem with system architecture and organizational maturity. From the complexity perspective, a co-evolution of system components is evident, as emerging

behaviors and new interdependencies motivate governance systems to change. Financial institutions are obligated to adapt dynamically and document responsibilities in matrices (e.g., Responsible, Accountable, Consulted, Informed (RACI) charts) and interface agreements to provide operational effectiveness with agility [60, 9, 70].

#### 6.3.2 Internal vs. External (Contractual) Boundaries

Complex financial IT systems often transcend service responsibilities beyond organizational borders. The introduction of contractual interfaces redefines how institutions allocate and manage operational control through outsourcing arrangements with multiple vendors and cloud services [112, 71]. As a result, the internal service ownership and external service dependency have become delineated and a focal point for modern ITSM strategies.

Integrating external service providers creates new interdependencies. Complexity theory suggests that cross-organizational interdependencies reduce control and increase system entropy [66]. This is particularly true in the financial services industry, where providers may have varying levels of maturity and compliance stances [5, 68]. Consequently, financial institutions have to manage “systems of systems”, where multiple autonomous agents interact and the outcome emerges from a single subsystem [81, 19].

To coordinate service delivery, frameworks such as Service Integration and Management (SIAM) have been adopted in the financial sector across multiple providers [72]. The ITSM has been extended to SIAMs with multi-sourcing environments by introducing integrator roles, standardized Operational Level Agreement (OLA)s, and SLAs that clearly define boundaries of control and escalation procedures. These techniques allow for local flexibility within globally consistent service delivery by acting as modular limitations in an otherwise dynamic system [49].

The simple presence of SLAs and formal contracts does not guarantee service coherence and delivery. As Russo et al. [96] emphasizes, IT quality management complexity increases when multiple vendors are involved in the service chain with different technological standards and change cadences. Service deterioration or non-compliance are frequently the results of misalignments between supplier capabilities and customer expectations. These emergent failure modes are exemplified by these phenomena that cannot be fully attributed to a single cause. Instead, the root cause lies within loosely coupled components [81].

Governance continuity becomes a concern due to contractual boundaries. Institutions operating in regulated environments must provide proof of resilience planning with meaningful audit trails and security controls to show compliance throughout the entire service stack, including third-party services [71, 112]. The regulatory frameworks, such as the DORA [46], reinforce this by explicitly holding financial entities accountable for cyber and operational risks posed not only in their organization but their service providers. DORA further distinguishes between Critical or Important Function (CIF)s and non-CIFs.

Complexity theory recommends using layered governance methods that adjust to shifting system topology and external interactions in order to cope with complexity issues. Centralized service portfolios with an integrated incident management protocol and ongoing service monitoring are examples of best practices in financial ITSM. Additionally, emerging technologies, such as the use of AI-enabled compliance engines and vendor risk models, are being used to dynamically monitor performance and mitigate uncertainty [110].

In conclusion, the growing reliance on external service providers in complex IT environments necessitates a reconfiguration of service management practices. Contractual interfaces and dynamic integration layers must be added to the traditional departmental or business unit boundaries. Complexity-aware service management must combine legal accountability with operational flexibility. This enables institutions to be adaptive while remaining compliant and resilient in increasingly complex systems.

### 6.3.3 Regulatory and Security Constraints on Responsibilities

Service management responsibilities in the financial sector are tightly interwoven with regulatory and information security obligations. Complex regulatory regimes and technical standards exist, and financial institutions are subject to them. These technical standards include the GDPR [44], the PSD2 [43], the DORA [46], and industry-specific frameworks like Basel III [13]. These rules restrict how operational tasks are organized and carried out, both inside and outside of organizations, in addition to defining compliance goals [112, 71, 19].

From complexity theory, the regulatory environment introduces constraints and feedback into the already established system. Financial IT infrastructures exhibit characteristics of CAS, which are emergent and non-linear. As a type of structural coupling, regulatory constraints shape acceptable system trajectories while adding to the cognitive burden of service managers responsible for control [81, 66].

In order to minimize fraud, error, or unauthorized access, SoD, a fundamental tenet in regulated IT settings, ensures that crucial tasks are divided across several roles. Complex IT systems and organizations have to enforce this rule across modular, distributed components, making the creation of roles and subsequent coordination and traceability especially challenging [70, 9, 100].

SoD can be operationalized through robust IAM systems that govern and report role boundaries across the dynamic and hybrid architectures [100]. IAM frameworks — including Role-based access control (RBAC), Attribute-Based Access Control (ABAC), and Privileged Access Management (PAM) — serve as enforcement layers within a complex system. These frameworks ensure that no single node holds unchecked controls over any systemic risk point [19, 112, 71]. As a result, informed design principles emerge, such as distributed authority with rule-based coordination and local enforcement with global visibility.

In order to manage complexities, they must coexist with emergent operational models such as DevOps and SRE, which emphasize automation through continuous delivery and decentralization. Particularly in complex systems, where localized actions can rapidly propagate through interconnected subsystems, the tension between agility and compliance is pronounced. Resultingly, organizations implemented “guardrail” architectures, which encode compliance policies directly into CI/CD pipelines and IaC templates to mitigate risks of non-compliance [72, 70, 37].

These adaptations illustrate a shift toward complexity-resilient governance structures. Compliance and security controls are being woven into the fabric of service orchestration, eliminating the need for manual oversight and allowing adaptive constraint enforcement without sacrificing responsiveness. This also aligns with complexity theories of self-regulating systems, where the behavior is not managed by a central authority but emerges through the interplay of rule-based agents operating within bounded conditions [40].

This challenge is further compounded by the complexity of cross-jurisdictional environments. Multiple legal and regulatory frameworks are reconciled by global institutions, with consistent access control policies and audit trails across all operational entities. Policies by local regulators have to be supported into the IAM system, but should still be integrated into enterprise-wide governance platforms, reflecting the multi-scalar nature of modern financial IT systems [60, 19].

In the management of complex financial IT systems, regulatory and security constraints on service responsibilities must be understood as both limiting factors and structural enablers. IAM and SoD mechanisms in the complex embedded environments, provide a foundation to guarantee compliance, trust, accountability, and system resilience. Not only does complexity theory account for the emergence of new risk patterns, but it also informs the design of adaptive governance structures that can scale with systemic interdependence.

#### 6.3.4 Interdepartmental and Business-IT Coordination

Due to the growth in complexity of the IT systems of financial institutions, service management can no longer be treated as purely technical or isolated operational functions. Instead, it must exceed the local functions and become embedded into the broader organizational structures, which encompass compliance oversight and business service delivery. These environments are akin to complex socio-technical systems, characterized by interdependencies among technologies, human actors, organizational silos, and institutional rules [99, 81, 19, 96].

In order to be effective in service management in these settings, collaborative governance mechanisms that allow IT, business, compliance, and risk management functions to jointly provide and own the IT service delivery outcomes are needed. Rigid hierarchies should be broken up and distributed control paradigms of complexity theory, which emphasize local adaptation and feedback-driven alignment, should be established [40]. In practice,

cross-functional structures with a trust-base, capable of responding to uncertainty and change, are the solution.

One approach is to designate a clear service owner and corresponding business owner for each service. The service owner oversees the service's overall performance and reliability, while the business owner focuses on ensuring it meets customer expectations and strategic objectives. The dual structure supports a clear local decision system without centralization to reflect a shared global outcome [9, 58].

Some organizations further formalize this relationship with a formalized role of Business Relationship Manager (BRM), as introduced in ITIL frameworks [9]. The BRM acts as a liaison between IT and business units, who translates service-level concerns into business-relevant metrics and vice versa. Although the title could be different, the function is a key coordinator in complex systems to bridge the perspective to the subsystem and resolve any friction among competing objectives.

In support of this, organizations are adopting shared responsibility models that delineate the functions into who is RACI across a service's lifecycle. These models serve as formalized dependency mappings, aiding in the management of complexity by rendering it visible and navigable rather than reducing it [60, 57, 70]. Therefore, complexity is not approached with simplicity, but rather with clarity and structure.

The introduction of governance boards or steering committees which span across Governance, Risk, and Compliance (GRC) and business domains was introduced into financial institutions. These entities offer a reflective capacity within the system, a venue for discussing systemic effects and weighing trade-offs. In complexity science, these forums are similar to boundary organizations, enabling sense-making across otherwise decoupled units [96, 19].

This structural alignment alone is insufficient; attention should be paid to cultural and temporal misalignments, such as differing planning horizons or incentive structures, which can undermine even well-designed coordination mechanisms. These challenges illustrate the non-linear nature of organizational behavior in complex systems, where minor misalignments can lead to systemic frictions. This requires shared goals with iterative feedback loops, allowing for common metrics. These principles are underscored in adaptive management frameworks and complexity theory alike [66, 70].

In summary, interdepartmental coordination must evolve from transactional hand-offs to adaptive collaboration with specialized roles for these functions. Complexity theory can explain why traditional hierarchical and monolithic silos fail, but support the design of shared accountability and responsibility structures with information and consultation exchange. This ensures service management is not only technically robust but also aligns with strategic goals.

## 6.4 Strategies and Methods for Managing Service Delivery in Complex IT Environments

### 6.4.1 Strengthening Core ITSM Processes and Governance

Complex financial IT systems and their ITSM require more than role clarity and organizational coordination; therefore, the ITSM processes must continuously evolve. Incidents and problems disrupt the backbone of ITSM and must be avoided with the specifically posed challenges of system complexity. Controlled change management could be the first approach to reduce incidents [70, 9, 13].

Mahalle, Yong, and Tao [71] describe this on applying ITIL processes in banking environments to handle operational risk. Traditional ITSM frameworks like this have emphasized the standardization of service processes to support efficiency and consistency for a long time. However, this is still insufficient for the application in highly complex and distributed systems with a higher demand for flexibility. The financial sector calls for tighter regulatory escalation, where incident and problem management must operate under stringent time constraints and auditability requirements. This requires the use of special ITSM tooling integrated into the systems with real-time monitoring platforms [112, 19].

Change management is a special challenge under the ITSM of complex IT systems that make coordinating change windows and evaluating the impact of changes intrinsically challenging [81]. A response to this is the transition from CABs toward more adaptive models that combine automation and risk-based approvals in their decision-making and accountability models. With these hybrid approaches, a higher level of release velocity with a maintained control over the provided changes [71].

The complexity theory sees these adaptations as a response to the non-linear and interdependent financial IT systems, relying on feedback loops and dynamic interconnections [66]. In these kinds of settings, deterministic models of process control are inadequate, hence it is necessary to create resilient and adaptable service management procedures.

Further, the requirement of business and risk management must align with the overall ITSM processes. Therefore, financial institutions are embedding operational risk metrics and regulatory controls directly into ITSM workflows. An example for this are, the incident priorities which are not just determined by the systems availability, but also the business impact and customer sensitivity [60, 96]. Problem management investigations yield the RCA, as well as evidence for any audit compliance and insights into the risk modeling. Therefore, integration of GRC platforms in the ITSM function is necessary, which measures against resilience and audit-readiness benchmarks [71, 58]. However, risks can differ fundamentally from those of simpler systems, where risks have to adapt to the changing conditions of complex systems.

Additional platforms are used by financial organizations to modernize their ITSM practices, notably Service Orchestration and Automation Platform (SOAP)s. These are able to

dynamically route tickets, automate remediation, and enhance reporting of the complex services. In critical and highly regulated platforms, automation is coupled with an embedded control logic to enforce compliance with SLAs [72, 70, 11].

Such adaptations unfold with real-world implementations, for instance, retail banks have replaced manual change approval processes with automated risk scoring systems. The score is assessed based on historical incident data and business impact [19]. Similarly, insurance companies under Solvency II [45] and Basel III [13] are introducing incident postmortem templates that align with internal audit requirements and ensure post-incident accountability and traceability [57, 9, 13]. Yet, such methods are themselves not without risks and can amplify unpredictable behavior or create blind spots. Hence, these approaches have to be complemented with mechanisms which ensure stability and resilience.

In conclusion, to strengthen the ITSM process, structural and technological innovation is needed. Institutions must transition from procedural compliance to outcome-oriented governance, which maximizes consumer trust and service stability simultaneously. This is underscored by complexity theory, which necessitates adaptive process designs and responsive governance to manage complex system behaviors.

#### 6.4.2 Automation, Monitoring, and Data-Driven Management

In complex IT systems, automation and observability have evolved from operational enhancers into essential elements of service management. The increasing number of interdependent services and third-party integrations renders human-led monitoring and response mechanisms inadequate for ensuring service continuity and regulatory compliance [70, 60]. There exists an increasing adoption of automation frameworks and advanced telemetry platforms to provide proactive and reliable service delivery.

Automation has advanced significantly in service management, currently extending beyond simple task scripting or run-book execution. Adopters have encompassed the application of AIOps, which leverages machine learning and big data techniques to correlate between alerting and predicting incidents with self-healing behaviors [18, 97, 1]. In financial institutions, which generate large amounts of structured and unstructured data from infrastructure, applications, network events, and user behavior, these capabilities are especially relevant.

AIOps platforms collect telemetry data from various layers of the stack and utilize statistical anomaly detection pattern matching to minimize noise and pinpoint actionable problems [1]. An example of this is an AIOps engine, which can correlate latency spikes in a trading application with a change of a downstream messaging queue, triggering an automated rollback to mitigate business impact. This not only supports real-time diagnostics but also helps with Post-Incident Review (PIR)s and continuous improvement loops [72, 71, 97]. Paradoxically, each automation or observability platform is itself another complex system which may reduce local fragility but increases global dependencies [66].

Observability has been another critical component for managing complex IT systems. Unlike passive monitoring, which only has predefined metrics and thresholds, observability provides deeper insights through distributed tracing by log analytics, and real-time dependency mapping [81, 19]. Unified observability platforms can offer end-to-end visibility across infrastructures, cloud-native applications, APIs, or vendor ecosystems. These platforms also improve metrics with faster identification of RCA and a reduction in Mean Time to Repair (MTTR). They are also able to improve compliance with SLAs [39].

In the context of complexity theory, observability serves as a vital facilitator of feedback control in systems. Traditional approaches fail to capture the behavior of non-linear interactions or anticipate cascading failures. Observability platforms improve the control and enable dynamic adaptations with more traceable indicators in complex IT systems [66, 81, 39].

Telemetry is the key to enabling this visibility. Logs are gathered in real-time, processed using stream analytics engines, and presented through dashboards customized for various stakeholder roles. Operations teams monitor systems and error rates, while a compliance team tracks audit logs and policy violations. With this role-based approach, the telemetry can ensure that service management decisions are made both timely and context-aware [60, 96, 57].

Data-driven management can be illustrated in the financial sector with the implementation of closed-loop remediation systems, where IaC policies are enforced by continuous compliance engines. These can automatically alert SOCs and prevent or revert unauthorized changes [11, 71, 97]. Institutions also have the option to adopt service reliability scorecards, which integrate observability data with operational risk indicators. This allows organizations to drive performance incentives and governance reporting [70, 18].

The true success of AIOps and observability platforms depends on the data quality and standardized schemas. Moreover, without appropriate oversight, excessive dependence on automation can hide systemic problems. Therefore, a balance between autonomous operation and transparent control structures has to be found, especially when compliance is another sensitive domain to be considered [19, 97, 58].

In summary, automation and observability are a transition into new strategic capabilities in managing complex financial IT systems. Complexity theory reinforces the need for these systems, which emphasizes the dynamic traits that complicate conventional approaches to service control in finance.

### 6.4.3 Organizational Structures and Sourcing Models

With the change to more distributed IT architectures, the organizational structure and sourcing models for service management have undergone a fundamental transformation [49]. The traditional characterized service offers, with a hierarchy over strict process governance and functionally siloed operations, are being challenged with agility and local ownership [70, 9, 11].

This evolution aligns with the broader complexity theory on CAS, where independent components respond to internal and external feedback and foster to emergent behaviors [66, 81]. These systems struggle to anticipate or control the non-linear service degradation and failure propagation. This led to the integration of ITSM directly into agile and product-based delivery teams, distributing decision-making authority closer to the operational edge and also integrating the responsibility [70, 19, 72].

Embedded models improve response time on incident resolution and change management, which strengthens the alignment between development outcomes and operational realities. In complexity science, it reflects the principle that local responsiveness is essential in these systems for the global behavior [40, 81]. In addition, modular organizational models minimize ripple effects across loosely connected units and isolate defects, hence reducing systemic fragility [100].

This shift is complemented with service reliability models, like the SRE and its domain-specific adaptation for finance published by Mina [78], Service Reliability Engineering (SvRE) [21, 70]. Such models emphasize certain techniques, which were already discussed as observability and automation. Service Level Objective (SLO)s with error budgets are another model which allows for control during uncertainty and high change velocity. SvRE uses these techniques for the risk and audit regulations of financial regulations. This integrates reliability practices with formal change control and compliance requirements [78, 6].

From the organizational and sourcing aspect, decentralization introduces new challenges. Complexity theory provides new insights into the structure of a system but warns against over-fragmentation. Coordination failures and emergent dysfunctions can occur when this exists [66]. In order to solve this, hybrid sourcing and organizational models are becoming increasingly popular. These models encompass decentralized teams fulfilling service obligations under a paradigm of limited autonomy, while a central service office maintains control over tooling, compliance enforcement, and process frameworks [19, 9].

Sourcing strategies can further compound system complexity. In financial institutions, this appears in hybrid environments, where internal services are outsourced to external vendors, who introduce new nodes into the service topology [60, 112]. These circumstances support the CAS idea that system-environment boundaries are dynamic and should be controlled via adaptive interfaces as opposed to rigid contracts [109, 81].

Therefore, many organizations have established Lead Service Integrator (LSI)s or adopted a SIAM approach. Within this approach, integrator functions orchestrate accountability and performance across the sourcing relationships of the organization [96]. The functions themselves have to be inherently dynamic and capable of absorbing shocks by realigning incentives and resolving ambiguity in ownership, all hallmarks in effective management of complex systems [49].

Evolving from technical and financial performance, sourcing governance has established new metrics and processes such as risk-informed vendor selection frameworks, dynamic contract monitoring, and regulatory fit analyzes, which should ensure that external

providers are reliably integrated into the service network [13, 46]. Other organizations are experimenting with newer sourcing models, such as dynamic models, where responsibilities can be reallocated based on real-time risk metrics and systemic stress. Strategies used in complexity management advocate for responsive and distributed adaptation [10, 19].

In summary, organizational structures and sourcing models in the financial sector are shifting. Effective service management has to integrate additional actors in their environment and adapt their organizational structures. Complexity theory offers insights on how these models could function with an emphasis on modularity and adaptivity.

### 6.4.4 Knowledge Management and Continuous Improvement

In the context of financial IT environments, knowledge is not only a critical asset but also a potential bottleneck. Due to the external and internal dynamics from an organization, a high rate of change needs to be expected. This aligns with the properties of CAS, where the system state is constantly reconstructed through interactions in the environment [66, 81]. Knowledge management is therefore not only about the storage of information, but rather enabling systemic adaptability and responsiveness.

To capture knowledge and documentation, centralized repositories and post-hoc reporting exist. Modern approaches practice Knowledge-Centered Support (KCS), which embeds knowledge generation into the service operations directly. As part of service delivery, teams continuously create, refine and apply documentation [97]. This ensures that, in addition to abstract policies and static documentation, information reflects real-time conditions.

An equally critical practice is PIRs. Since failures cascade over multiple system elements, an extensive review can create an opportunity to learn and redesign actions the next time [21, 70]. In the financial sector, this also serves the compliance function used in audit trails and can demonstrate organizational learning to the supervisory bodies.

Feedback mechanisms allow systems to adjust dynamically in response to performance signals and anomalies. Feedback loops manifest in telemetry-informed change controls and user experience metrics, which influence the service design and link to dashboards [66, 96]. A formalization of feedback loops is achieved through tooling and governance structures which capture and act on knowledge across technical boundaries and the whole organization.

Digital tooling can be in different forms: observability platforms, integrated ITSM suites, version-controlled wikis, and AI-supported knowledge assistants. Spoken in complexity terms, these platforms allow for improved observability, enhance actor coordination, and reduce time-to-adaptation [81, 97]. One requirement is for the systems to account for socio-technical dynamics, so that human and machine actors can access and interpret information to a point which is relevant to their role in the service ecosystem [99]. The organizations need a learning culture, which emphasizes, knowledge exchange and growth. The learning culture should reward experimentation and promote knowledge sharing across silos [70].

To conclude, knowledge management and continuous improvement are the foundation to management in complex systems. They should work as memory and nervous systems, where institutional knowledge should be preserved, while adaptive controls should be enabled. With an alignment of documentation practices and feedback mechanisms, responses to the systems can be better executed. It also reduces the likelihood of repeated failures and continuously evolves service management practices.

### 6.4.5 Legacy System Integration and Technical Debt

Legacy systems and their integration into newer technologies are one of the most persistent and complex challenges in financial ITSM. Despite the adoption of cloud platforms and newer technologies in the sector, many core services — particularly in banking and insurance — still depend on older mainframes, batch processing logic with proprietary protocols [3, 96]. Legacy elements have significant constraints on agility. The coexistence of modern and legacy technology stacks increases not only system complexity but also operational fragility.

According to complexity theory, financial IT ecosystems are multi-layered socio-technical systems with path dependency and historical coupling, which in turn provide unequal rates of change [99, 66, 81]. These legacy systems often form the “deep structure” and act as a core of critical nodes which resist modification due to their high transformation cost and organizational inertia. Overall, unpredictability often originates from the opacity of these systems [40].

A commonly referred term for this dynamic is technical debt, which is the accumulated cost of deferred modernization that increases the risk of cascading failure [24, 33]. Technical debt is an organizational and architectural issue apart from being a technical artifact. Unmanaged technical debt can limit system modularity and raise the risk of brittle service interfaces in complex contexts. This also relates to the Cost of Delay (Cod) model, which highlights the economic consequences of postponing modernization initiatives [94].

Several integration and modernization strategies have been employed in the technical sector. A common approach is abstraction layers, which encapsulate legacy systems behind APIs or service buses. Thereby, direct dependencies are reduced and more modern service interactions are possible without a complete re-platforming [10]. This strategy promotes modular governance, which is based on the complexity theory that strongly coupled subsystems should be segregated to maintain service continuity and avoid cross-system interference.

A second strategy is the gradual modernization, where a legacy component is incrementally replaced over time. This can be implemented through strangler patterns, containerization of legacy services, or phased microservice decomposition [31]. By allowing systems to evolve through safe-to-fail experimentation and local optimizations, rather than top-down replacement initiatives, they follow the complexity-based approach of adaptive transformation. This approach is better suited to handle scale and unpredictability.

Some organizations also adopt service encapsulation strategies, where legacy logic is maintained but surrounded by enhanced observability and compliance wrappers. For instance, organizations may wrap COBOL batch jobs with scheduling and monitoring tools, or use Robotic Process Automation (RPA) to simulate modern interfaces on legacy user terminals. While such measures may not eliminate technical debt, they mitigate its operational risk and support regulatory traceability [60].

However, the downside of abstraction strategies is that one cannot mask complexity and expect it to disappear — it merely shifts complexity to another part of the system [66]. A layered workaround can, over time, create hidden interdependencies and reduce transparency. Therefore, when one of these approaches is chosen, it should be accompanied by systemic observability, such as dependency mapping and behavioral monitoring [72, 19].

There are organizational ramifications to legacy integration, as an increasingly small number of experts possess the tacit knowledge needed to maintain and fix older systems. This introduces a people-centric fragility; knowledge loss can occur due to retirement or attrition which in turn undermines service stability. Key enablers for this include effective knowledge management and succession planning [70].

To summarize, the existence of legacy systems and modern technologies is one of the defining features of complex financial IT systems. Technical compatibility requires more than managing this coexistence; it demands an adaptive, complexity-aware service management strategy focused on modularity and incremental change. Institutions are better able to maintain service continuity, lower systemic risk, and adapt to changing market and regulatory needs when they approach modernization as an ongoing, system-wide learning process.

### 6.4.6 Service Recovery and Crisis Management

While incident management and PIRs are important, service recovery demands more than procedural incident handling. It requires more resilience-oriented strategies, that accommodate the uncertain behaviors of these systems [81, 66]. Increasingly, financial institutions function in digital ecosystems where failures can spread unpredictably and originate from opaque dependencies across technological and organizational barriers [19, 70]. Instead of being a standalone function in such systems, crisis management becomes a systemic competence.

Central to a capable recovery and crisis management are incident recovery playbooks. Playbooks are codified escalation paths with fallback options and communication routines; this enables distributed teams and crisis units to coordinate under time pressure or uncertainty [72, 97]. These artifacts function as operational scaffolding for decision-making, when signal-to-noise ratios are low and judgments must be made in real-time with incomplete information.

Effective recovery also hinges on learning from disruptions. The RCA has traditionally been used to identify the origin of incidents. In complex systems, the notion of a single

root cause is often reductive. Multi-causal, systems-thinking viewpoints that see incidents as the result of interactions between technical and human variables are becoming more prevalent in modern approaches [66, 81]. The SRE and DevOps cultures have established post-mortem practices that emphasize understanding systemic factors over attributing fault to individuals. These reviews not only help with operational learning but also satisfy audit and compliance requirements.

Service resilience has also anticipatory practices in place, such as DR drills, fault injection, and penetration or stress testing. The goal of these simulations is to expose fragilities and train response teams in handling black swan scenarios [31]. This allows them to assess how their systems deteriorate under harsh circumstances and to enhance failure containment tactics [14].

Processes known as lessons learned formalize the integration of post-incident insights into the broader organizational culture. They vary a lot from updates to change management procedures or revisions of SLOs and architectural patterns. These feedback loops of continuous improvement are increasingly integrated into ITSM platforms [96, 60].

From the perspective of complexity science, crisis management and service recovery demonstrate the necessity of learning-oriented and adaptive control systems. Centralized crisis teams may lack the necessary experience or speed to respond appropriately in high-complexity situations. Instead, resilient recovery requires empowering actors with autonomy and clear guidance to detect and respond to disruptions in real-time [30, 54]. Thus, systemic readiness has to be built into the service architectures and governance frameworks of institutions.

In summary, managing service recovery in complex financial IT systems involves more than reactive incident resolution. Anticipation and preparation should be implemented in organizational routines. Institutions that systemize these practices and carry out continuous learning in their tasks are able to reduce downtime and reputational damage.

## 6.5 Assessing the Effectiveness of Service Management in Financial Institutions

### 6.5.1 Operational KPIs and Metrics

Traditional service management metrics will still have an essential role in complex financial IT systems, but fail to capture the full spectrum of operational effectiveness. These metrics include system availability, MTTR, incident volumes, and SLA compliance, which provide an important baseline but tend to reflect only the surface-level performance. However, a wider and more dynamic collection of indicators is required due to emergent behaviors through cross-domain interaction and non-linear failure propagation [81, 66].

According to complexity theory, systems characterized by interconnectivity and dynamic behavior need more than static and siloed metrics. An SLA may attest to the uptime compliance of a single component while neglecting to account for the worse customer

experience brought on by sluggish interactions across loosely linked services. Similar to this, MTTRs track restoration time, but cannot depict how resilient or adaptive the recovery process was [30, 54].

The gap created can be supplemented by complexity-aware performance indicators, these include resilience metrics—such as recovery time variability, system stress thresholds, and incident recurrence rates. They capture system performance under normal conditions, as well as adaptations under pressure [66, 54]. CAS uses such metrics to serve as proxies for systemic health and adaptive capacity, rather than isolated component reliability.

Other emerging categories involve experience-based metrics, such as eXperience Level Agreement (XLA)s, Net Promoter Score (NPS), and customer satisfaction indices. User-perceived service quality becomes the primary focus as a metric, rather than relying solely on technical performance Vargo and Lusch [113]. Despite their inherent subjectivity, they are crucial in settings where value is determined by service integration and interaction quality [19, 70]. Complexity theory supports this view; users and stakeholders who interact with the system under diverse conditions depend on feedback from distributed agents in the global outcome of CAS [109].

Additionally, leveraged composite or multi-dimensional indicators combine operational and experiential measures. SLA violations may be weighted in service quality indices according to their anticipated financial or reputational ramifications. In frameworks like DORA, which demand institutions to not only show baseline compliance but also the capacity to provide vital services both during and after disruptions, are in line with the regulatory push for operational resilience [71, 112].

With automation and telemetry, a real-time KPI dashboard could be created and customized for different roles. Operations staff may monitor error rates and latency; risk officers may track incident trends and policy violations; executives may review customer satisfaction and regulatory exposure. A role-based observability supports decentralized decision-making while maintaining global alignment, which is considered an essential governance mechanism in financial institutions [97, 81].

Yet, as complexity theorists warn, oversimplification of metric design can become a risk. Masking of hidden interdependencies or the creation of a false sense of control, are examples of this. A team which optimizes for low incident count may delay reporting or over-automate resolution, suppressing valuable signals. As Snowden and Boone [103] argue that in complex domains, metrics should guide sense-making, not control decisions.

Some institutions are using adaptive metrics, where performance indicators are periodically reassessed, based on the dynamics of a system and risk profiles. The complexity-aware governance principle aligns with these practices.

To sum up, operational KPIs in complex financial IT systems should expand beyond conventional service level indicators to include adaptive capacity and user experience. Rather than serving merely as tools for compliance, metrics should aid in learning and

feedback. Complexity theory warns against reductionism and provides a road-map for the design of performance indicators, which reflect the true nature of dynamic services.

### 6.5.2 Monitoring Practices and Reporting Tools

The monitoring of complex financial IT systems consists of passive observation to active sense-making across the whole landscape. Traditional monitoring focused on passive systems built around discrete alerts and static thresholds monitored in siloed dashboards. With the increase of organizational and technical complexity, this remains insufficient [108, 81, 66, 54].

CAS theory uses observability as a precondition for adaptive management. This can translate to the deployment of monitoring infrastructures that can provide real-time, context-aware insights. This monitoring software should be able to include all various systems across the whole IT [19, 96]. The requirements for monitoring should also support horizontal visibility, across services and platforms, as well as vertical traceability from infrastructure components up to business-facing outcomes [116].

Telemetry data is becoming the cornerstone of monitoring [72, 97]. Each layer of the technology stack must continuously collect data and further process it via analytics engines that detect anomalies and correlate events for actionable intelligence information. Distributed sense-making — where agents (human or automated) interact with real-time signals to adjust system behavior in response to perturbations — is supported by this architecture [66, 81].

Complexity-aware monitoring tries to integrate technical and business-facing metrics. Traditional infrastructure performance (e.g., CPU load, memory usage) often lack strong user experiences and timely business outcomes. Financial institutions integrate additional indicators such as Service Level Indicator (SLI)s and XLAs, which provide meaningful business process telemetry into unified observability platforms [96, 97].

The complete toolchain which implements these practices varies, but generally includes a combination of open-source platforms (e.g., Prometheus, Grafana, Elastic Stack), commercial observability suites (e.g., Splunk, Dynatrace, Datadog), and custom-built telemetry pipelines. In order for the monitoring to be actionable across domains, these systems can be integrated into ITSM systems and dashboards [70, 97]. Integration encompasses both technical and epistemological dimensions. Moreover, information should be conveyed in formats that allow decision-makers to interpret and act effectively within their specific functional contexts [93].

Monitoring should not create the illusion of total visibility, as blind spots and latent interdependencies are inevitable. Therefore, more resilient monitoring practices include meta-observability—monitoring, which monitors the monitoring system itself [66]. This second-order feedback allows institutions to identify when monitoring is outdated or insufficient with the evolution of the system [39, 93].

In summary, monitoring must evolve from a reactive instrument to a proactive, adaptive observability tool. Toolchains must support distributed cognition and align across functions. Service management strategies should include role-based perspectives over multiple layers and ongoing validation of monitoring efficacy.

### 6.5.3 Compliance, Risk, and Audit Alignment

Compliance, risk management, and auditability are other factors to integrate into the service management of complex financial IT systems [46]. The operational framework of ITSM must incorporate regulatory standards due to the structural and behavioral features of large adaptive systems, including non-linear risk propagation [81, 66, 19]. Compliance and risk controls have to evolve endogenously in the system and dynamically adapt, while still supporting governance mandates.

ITSM is the primary factor in which financial institutions operationalize regulatory obligations such as those imposed by GDPR [44], PSD2 [43], DORA [46], MiFID II [42], and Basel III [13]. ITSM processes offer traceable paths to especially change management, incident response, and problem tracking [71, 112, 19]. These procedures serve as the cornerstone for audit trails and risk accountability across federated architectures when combined with IAM, Configuration Management Database (CMDB)s and their automatic logging systems [60, 70].

Risk can arise from the interplay of complex system components under various circumstances, rather than due to specific failure sites [30]. Deterministic compliance models or risk registers fall short in complex IT systems. Therefore, institutions have increasingly embedded risk-based KPIs and resilience indicators into their ITSM dashboards. These metrics include change failure rates, blast radius estimates, time-to-detect anomalies, and cross-system dependency risks [96, 97].

Auditability has its own complexity-aware approaches. Central audit mechanisms lack contextual relevance or real-time visibility. ITSM platforms have adopted continuous compliance by integrating automated documentation and immutable logs. They are also integrating version-controlled workflows and role-based policy enforcement [9, 19]. Institutions may maintain audit preparedness without sacrificing operational agility due to these capabilities, which also lower the overhead associated with human evidence collecting.

Adaptive or automated compliance mechanisms also exist. They use technology such as policy-as-code for managing policies using code and just-in-time access provisioning. One more mechanism is automated exception handling. This allows localized rule enforcement that is observable at the system level [72, 66]. In multi-jurisdictional settings, where regulatory requirements vary by location and need to align under a single governance framework, these methods are especially crucial.

Diverse business sectors need cultural coordination in the organization, and so does the financial sector. The shared awareness of risk across teams is as important as

cross-functional alignment between compliance officers and service managers. Risk and audit processes should be integrated into day-to-day operations. This is supported by complexity science, which highlights the value of collaborative governance and distributed sense-making in systems with decentralized knowledge and control [105, 40, 109].

The alignment of compliance, risk, and audit requirements with ITSM requires complexity-informed governance practices that embed regulatory logic into operational workflows and support auditability through continuous, automated documentation. In the face of systemic instability and change, this permits both adaptive resilience and legal compliance.

#### 6.5.4 Qualitative Feedback and Stakeholder Perspectives

Organizations remain focusing on quantitative indicators, which prove insufficient for evaluating service management effectiveness in complex systems, therefore qualitative feedback becomes a critical input [81, 109]. Institutions can better understand system behavior in context and adapt to changing needs by gathering stakeholder opinions through participatory governance forums and structured feedback loops [99].

Complex systems are characterized by decentralized knowledge and distributed controls, where no singular actor has complete knowledge of system performance or risk exposure [105]. Therefore, it is necessary for various stakeholders, such as IT operations, business units, customer service, compliance, and external partners, to have ongoing conversations in order to co-create service quality and system resilience [83, 40, 19].

Service review boards and stakeholder advisory councils are examples of business-facing feedback loops. These business-facing feedback loops enable the integration of experiential knowledge into ITSM practices. Lived operational experience is a tool for reflective learning on an iterative update base [30, 70]. An example that is essential for meaningful service improvement is customer-facing teams, which may report on usability bottlenecks or client dissatisfaction that are not captured in system logs or KPIs.

Furthermore, the identification of latent system vulnerabilities that have not yet caused incidents but could, in certain circumstances, require qualitative insight. Due to their frequent exposure to system touchpoints, frontline operations personnel and customer support representatives are frequently the first to notice indications of performance drift or usability issues [96, 99]. Complexity theory suggests these weak signals may precede systemic stress and should inform adaptive planning mechanisms [84].

Service postmortems and retrospectives offer an opportunity to integrate qualitative input. These forums assist in revealing hidden dependencies and process misalignments that may go undetected by quantitative measurements when they are set up as open, non-hierarchical debates [21]. This form promotes knowledge exchange and reduces repeated failures.

Regulatory expectations also often include “soft” criteria such as governance maturity and evidence of proactive service management, which is ensured through qualitative assessments. Incorporating compliance stakeholders into feedback procedures guarantees

that service modifications take into account changing audit expectations and regulatory interpretations, in addition to technical or business requirements [112, 71].

Within complexity-oriented services, stakeholder perspectives provide decentralized and valuable observations that collectively reveal the behavior of the broader system. It takes procedural and cultural conditions, such as psychological safety and open lines of communication, so that a criticism can be used as responds to improve the system [70, 97]. It should be set up so that feedback is treated as a primary driver of service adaptation instead of reactive commentary. This allows for alignment with the system's needs.

In conclusion, stakeholder interaction and qualitative input are essential elements of ITSM. These elements enhance observability and enable adaptive governance, which in turn support organizational learning. By institutionalizing cross-functional feedback loops and stakeholder reviews, complexity can be managed by embracing it as a source of operational insight and strategic flexibility.

## 6.6 Preliminary Reflections and Synthesis

### 6.6.1 Preliminary Reflections on RQs

The preceding literature analysis offers insights into how financial institutions are adapting service management practices to accommodate the increase in system complexity. Several patterns have been identified that inform the RQs of this thesis. These observations serve as a conceptual link between the theoretical underpinnings and the impending expert interview-based empirical investigation.

First, the complexity of financial IT systems is mainly shaped by the choice of success metrics and their interpretation. Metrics used in non-complex systems are still widely used, but increasingly being complemented by experience-level indicators, resilience measures, and feedback-driven performance reviews [70, 60]. This change is consistent with complexity theory's focus on emergent outcomes and adaptive feedback loops. However, in existing literature, a consensus is missing on measures to holistically assess effectiveness in complex services, particularly when resilience and user experience trade-offs are involved [30, 97].

Second, foundational tools for managing complex systems use automation and observability. Enablers are platforms that enable telemetry ingestion for anomaly detection and real-time decision-making (e.g., AIOps, self-healing infrastructure) of adaptive service delivery [97, 81]. Yet, limited insights are given into the organizational readiness factors and governance adaptations required to scale these tools in regulated financial environments. Questions remain on how organizations integrate automated decision-making into complex service architectures without introducing opaque or uncontrollable procedures, as well as how they strike a balance between automation and auditability [19, 96].

Third, the adoption of strategies appears to be highly contextual. Some organizations use hybrid models that maintain centralized control over compliance and process standardization, while others completely integrate SRE or decentralized DevOps principles [72, 21]. In the literature, the recommendation is based on approaches that acknowledge the complex, socio-technical nature of financial service ecosystems—adapting governance models and tooling landscapes to system-specific constraints [99, 40, 109]. However, little actual empirical evidence comparing strategies across different organizations within the financial sector is present.

Based on these observations, several hypotheses can be formulated for exploration in the expert interviews:

- **H1:** In complex financial IT systems, the incorporation of continuous improvement metrics (e.g., frequency of PIRs, learning velocity) and experience-based metrics (e.g. XLAs, customer satisfaction), in addition to traditional technical metrics (e.g. uptime, MTTR), provides a more holistic measure of service performance than relying solely on technical indicators.
- **H2:** Multi-layered monitoring (e.g. real-time telemetry, role-based dashboards, event-driven alerts) proves more effective in capturing the full spectrum of service performance. This leads to stakeholders evaluating these metrics more favorably than static or siloed approaches in the service management of complex IT environments in the financial sector.
- **H3:** In non-deterministic complex IT systems in the financial sector, where behavior cannot be fully predicted or reproduced, adaptive monitoring and quality assurance practices (e.g., dynamic SLOs, anomaly detection, resilience engineering) are more successful in maintaining service quality and operational control than those relying on deterministic models.
- **H4:** In the service management of complex financial IT systems, automation and monitoring tools that embed security and compliance checks (e.g., “policy as code,” automated compliance gates) significantly enhance release velocity and reduce risks.
- **H5:** Financial institutions that approach legacy-system modernization as a continuous, feedback-driven strategy, rather than one-time transformations, achieve more robust service management outcomes and reduce technical debt over the long-term on highly complex IT systems.

These hypotheses reflect gaps and assumptions in the literature which require empirical validation. The expert interviews will specifically investigate how practitioners operationalize complexity, how emergent behavior and uncertainty impact strategic choices, and what trade-offs are made to strike a balance between agility, control, and compliance.

## 6.6.2 Summary and Transition to Interviews

The chapter has delved into the management of financial IT services within complex and socio-technical environments. The investigation, which drew from a wide range of scholarly and regulatory sources, showed that contemporary service management needs to adopt flexible, complexity-aware tactics.

Important takeaways include the significance of distributed responsibility models, how automation and observability facilitate responsive control, and the increasing necessity to balance system adaptability and regulatory compliance. The chapter also highlights the importance of stakeholder feedback loops and how knowledge-sharing frameworks are used and integrated into systems.

Complexity reshapes fundamental assumptions, including those about reliability and performance. Linear processes are increasingly being replaced by dynamic ones that can accommodate emergent behaviors and feedback effects. While frameworks like ITIL remain relevant, they require adaptations in the form of flexible tooling which incorporate cross-functional collaboration, and cultural alignment.

While conceptual models are manifold, the literature review identified several areas in which empirical understanding remains limited. For instance, whereas automation is generally seen as a crucial facilitator of resilience, its application in compliance-focused settings is not well defined. Comparing hybrid sourcing models and decentralized responsibility schemes across institutions and dealing with comparable complexity concerns.

The transition from theoretical analysis to qualitative inquiries will allow the following expert interviews to validate or challenge the preliminary reflections outlined above. The understanding and management of complexity in practice, the selection and institutionalization of adaptive methods, and the operational evaluation of service resilience will all be covered in these interviews. Ultimately, the empirical phase aims to uncover how financial institutions translate complexity theory into actionable processes.

# Interviews

## 7.1 Introduction

This chapter presents the results of six expert interviews conducted to explore service management practices in complex IT systems within the financial sector. The goal of the interviews was to gather first-hand insights into how complexity is managed in ITSM operating in the financial sector. The interviews particularly focused on legacy systems, regulatory demands, automation, metrics, and monitoring. A thematic analysis was conducted to evaluate the statements, combining both deductive and inductive coding techniques. The results are organized into eight overarching themes that surfaced from the interviews and serve as empirical foundations for the research.

## 7.2 Interview Overview

### 7.2.1 Participant Profile

Seven individuals participated in six semi-structured interviews, which were conducted over two rounds. The first round included an interview with two experts from the same organization. This resulted in three interviews per round. All interviewees held senior positions within the financial sector in Austria and possessed at least 5 years of experience. Multiple domains were covered, including software engineering, IT operations, risk management, regulatory compliance, and information security. The organizations which participated in the interviews included major institutions in the banking, insurance, capital market infrastructure, and payment services fields.

The interview partners are anonymized and referred to as Interviewees A to G. Table 7.1 provides an overview of their roles and the sectors they represent.

Due to better knowledge transfer, all interviews were conducted in German and took place with participants based in Austria. Nonetheless, it is important to note that many

Table 7.1: Overview of Interview Participants

ID	Position	Organization Type	Round	Interview
A	Managing Director responsible for software engineering	Insurance	1	A
B	Head of IT Projects & Services (Software Development)	Capital market infrastructure	1	B
C	Senior Risk Manager and IT Governance Lead	Capital market infrastructure	1	B
D	Head of IT Operations (formerly Service Management)	Banking	1	C
E	IT Systems Specialist in Digitization Projects	Payment services	2	D
F	Head of Outsourced Product Development and Technical Vendor Management	Financial software development	2	E
G	Chief Information Security Officer (CISO)	Insurance and banking	2	F

of the represented companies operate internationally. The insights of the interviews were later translated into English to maintain the form of this thesis. The participants' backgrounds span over various areas within the financial industry. This shall ensure a broader view of practices across the sector, with a diverse view and a representative set of perspectives. No autodidactic or unstructured interviews were conducted. In addition, the interviewer's professional expertise in IT governance and service management in the financial sector contributed to a context-aware yet neutral moderation.

### 7.2.2 Interview Procedure

Every interview used a semi-structured framework based on an interview guide. The duration of the interviews ranged from approximately 45 minutes to one hour. Four thematic sections guided the interview: (1) introduction and context setting, (2) complexity in IT systems, (3) hypotheses and topic-specific questions, which were further split up into the individual hypotheses, and (4) reflective and exploratory closing.

The interviews were conducted in two rounds. The first round aimed to examine the general framework and procedures of service management in complex financial IT systems. The guide was applied uniformly across three interviews, which allowed for initial comparisons and the identification of emergent themes.

Based on the first-round findings, the guide for the second round was refined. The structure stayed the same, but the questions became more focused and partly more quantitative in nature. The second round aimed to clarify open questions, explore missing or ambiguous information, and examining new topics raised by earlier participants (e.g., RegTech or change management).

Two interviews were conducted remotely via video conferencing, while the remaining four took place in person at the participants' offices. Prior to the interviews, each participant provided their written informed consent that included explicit agreement for audio recording. In every instance, a signed statement of consent was acquired.

After each interview, the audio recording was stored and transcribed. Later, it was imported into MAXQDA for qualitative data analysis. To guarantee correctness and prepare the transcriptions for structured coding and interpretation, the automated transcription was manually proofread with quality control.

### 7.2.3 Method of Analysis

#### Analytical Framework

The interview data were analyzed using thematic analysis, following the approach defined by Braun and Clarke [26]. This method is suitable for identifying, organizing, and interpreting themes across qualitative datasets. As the research implements experimental and theoretical elements, it led to the adoption of a hybrid strategy that blends deductive and inductive coding techniques [47].

Deductive codes were derived from the interview guide and the predefined research hypotheses, while inductive codes emerged directly from the interviewees' responses. This dual strategy is structured and enables a comparison along the key thematic dimensions (e.g., metrics, monitoring practices) and the exploration of recent insights (e.g., references to emergent behavior).

The analysis was conducted manually, aiming to capture the frequency and perceived relevance of themes. The relevance of themes was determined by the frequency of concepts mentioned and the emphasis placed on them by participants. This process established a focused analysis through triangulation of theoretical assumptions, interviewee experience, and practical relevance.

#### Coding Process

Following the transcription, all interview data were imported into MAXQDA for qualitative analysis. An initial codebook was developed using a combined deductive–inductive approach: top-level codes were derived from the interview guide (e.g., “monitoring,” “automation,” “legacy systems”), while additional codes emerged iteratively from the data during open coding (e.g., “time to market,” “predictive maintenance”).

The coding process followed two cycles; first, descriptive and conceptual codes were applied to individual meaning units across transcripts. Second, thematically related codes were clustered into higher-order categories through focused coding. Where applicable, axial relationships (e.g., between causes, conditions, and consequences) were identified to uncover deeper structural patterns, although the overall analytical approach remained thematic rather than grounded-theoretical.

Following the formation of thematic clusters, each individual statement was compared across participants to identify recurring patterns, contradictions, and sector-specific nuances. A total of 79 key statements, each characterized by either high frequency or high perceived relevance, were found and assigned unique identifiers (e.g., K11, K23). These are referenced throughout the findings to ensure traceability between empirical data and thematic interpretation.

The coding and analysis process was informed by established methodological guidance for thematic analysis from Braun and Clarke [26] and Nowell et al. [88]. This should emphasize particular attention to transparency and replicability, as well as alignment between data, codes, and analytical conclusions. A complete list of the coded key statements is provided in Appendix 9.

## 7.3 Emerging Themes

### 7.3.1 Theme 1: Structural and Socio-Technical Complexity

The first theme identified from the qualitative data underscores the inherent structural and socio-technical complexity found in financial IT services. Participants referred to a landscape shaped by technological heterogeneity (K1, K64) characterized by the co-existence of different systems, such as a core software product, legacy stacks, SAP, and DevOps. This hinders the development of a standardized approach and amplifies unintended side effects. The technical challenge is further amplified by organizational factors, which can create disconnects and fragmentation, ultimately leading to role ambiguity (K2, K18). For example, overlapping responsibilities and decentralized structure complicate coordination and decision-making.

Legacy systems were described not simply as central and technologically outdated systems, but also as embedded structures with cultural, operational, and economic inertia (K11, K26, K41). Attempts to modernize such systems, through different strategies, such as modularization (K73), parallel systems (K72), microservices (K8), or selective transformation, frequently collided with conflicting internal and external stakeholder agendas (K12, K45). Simultaneously, their continued use is justified by their stability, compatibility requirements, and embedded knowledge.

Partner ecosystems, from third-party contributors, further increase complexity. The presence of multiple vendors, third-party providers, and shared governance structures — both within and across institutional boundaries (K16, K31, K45) — introduces coordination challenges that extend beyond technical barriers that require management of political and contractual domains. Often, system architectures are shaped as much by the technology itself as by organizational dynamics. Literature refers to this phenomenon as socio-technical systems, which are a hallmark for organizations (K46, K62).

The influence of technological trends and strategic tensions is also highlighted by some interviewees (K27). These include the cyclical shift in infrastructure towards cloud and on-premises solutions, the trade-offs between explainable decisions and fast automated

decisions by AI, and the impact of standardization initiatives by holding companies. This evolving relationship between local autonomy and central governance (K63) suggests that complexity is not static, but is dynamically reconfigured by institutional and strategic decisions.

In summary, socio-technical complexity in financial IT systems and its structures is the result of scale or technical sprawl. Nonetheless, it emerges from the entanglement of different technological and organizational drivers, such as cultural, regulatory, business, and operational complexities. Legacy constraints, institutional roles, stakeholder heterogeneity, and strategic tensions are examples of these drivers. These dynamics pose the foundational challenges for effective service management and require adaptive, context-aware mechanisms which transcend traditional IT control models.

### 7.3.2 Theme 2: Monitoring Practices and Observability Limitations

The second theme centers on the practices and limitations of monitoring in complex financial IT systems. Across the interviews, gaps in systemic visibility and fragmented monitoring infrastructures emerged as recurring concerns. The results produced by monitoring solutions often result in isolated views or “island monitoring”, even though most organizations monitor at least the application and infrastructure layers (K4, K6). This leads to a lack of integrated observability across service boundaries.

Multiple institutions have adopted multi-layered monitoring dashboards and logging architectures with configurable depth and also designated them as this (K21, K67, K68). This allows for dynamic adjustments in log granularity and visualization of transaction paths, as well as adaptive strategies depending on different factors of the system or its environment (K36). However, interviewees emphasized that these tools are mostly monitoring a technical scope and often fail to deliver an impact analysis across domains or a user-centric view (K37, K48). While most institutions use customer-based metrics, they struggle to convert these metrics into meaningful measures to improve the service experience, especially when the relationships are B2B (K5, K35).

Another issue is the reliance on availability and incident-based KPIs (K65) as primary indicators of system health. While these metrics are clear, they can mask emergent or degraded service states—especially when the availability remains high, as the KPIs indicate, but the user experience suffers due to other service issues. One respondent described this as “the illusion of precision”, which was also salient in post-incident analyzes (K66), where root causes were sometimes constructed more to reassure management than to reflect technical reality.

Some organizations made selective progress on adaptive monitoring of services and anomaly detection (K22), especially on security services and/or performance-focused contexts (e.g., SOC Radar, latency dashboards). These approaches are often only domain-specific, particularly when looking at security, and rarely feed into an overarching complexity-aware monitoring model. The trade-offs between data retention and data volumes have been mentioned in this context as well.

Overall, the analysis suggests that monitoring is mostly reactive and often siloed due to lack of sufficient contextualization. There is a desire for an environment where predictive analytics are provided in the context of predictive maintenance over historic patterns (K54). However, this maturity is currently not feasible, and it remains unclear if this state can ever be achieved. While isolated innovations are present, a lack of true end-to-end observability, user-centered impact metrics, and adaptive systems, represents a significant blind spot in the current service management of complex IT environments.

### 7.3.3 Theme 3: Automation – Opportunities, Risks, and Control Challenges

The third theme focuses on the dual nature of automation in the service management of complex IT systems. On the one hand, automation can increase efficiency and reproducibility or standardize processes, while on the other hand, participants pointed out that unintended side effects and operational limits with contextual fragility exist.

It was described that mature automation practices exist in areas such as deployment pipelines, testing, security and infrastructure provisioning (K23, K53), often implemented through internal DevOps platforms, SOAR solutions or AIOps. Although these initiatives promote speed and consistency, they also necessitate a large investment in dependency mapping and architecture-aware design. Several experts emphasized that it often relies on an accurate service dependency model to be effective (K53, K54).

Concurrently, respondents noted multiple constraints and risks. Automation may lead to more rigid workflows that fail to handle exceptions (K7) or produce harmful effects when over-applied without fallback mechanisms (K24). Rather than reducing complexity, automation often shifts it to another part of the system. “More code, more expense, more maintenance, more risks” was one quote mentioned during an interview. A cost-benefit curve can help determine how much automation is beneficial for the current system (K55).

Additional concerns arise in high-stakes or regulated environments, where it was noted that human oversight remains necessary (K25). Some organizations enforce manual checkpoints (e.g., four-eyes principles) to preserve situational control (K24). False-positives in rule-based systems also can pose challenges (K69), by potentially overwhelming incident handlers or triggering erroneous interventions. Although AI-based optimization (K76) and adaptive automation (K14) were mentioned as promising mitigation strategies, they remain limited in scope and maturity.

Interestingly, one participant reported minimal or cautious automation adoption (K39, K40), particularly in contexts where institutional risk aversion, legacy constraints, or regulatory uncertainty dominate. While automation tools exist, their usage is often fragmentary or informal. This could also be due to cost considerations in the context of automation tools, such as relying on robocalls instead of integrated alerting systems (K40).

In addition, automation involving AI or machine learning components (K13, K43) raises further issues around transparency and explainability. In complex service contexts, the possibility of losing situational awareness provides a challenge to greater integration and trust.

Altogether, this part illustrates that while automation is a valuable enabler, its deployment is neither trivial nor risk-free. While all interviewees view automation and AI as a technological trend and opportunity for the future, the maturity for more autonomous systems than those described has not been reached yet. Effective automation in complex IT systems requires robust infrastructure and clear policies, while maintaining an understanding of its limits, side effects, and the contexts in which human judgment remains indispensable.

#### 7.3.4 Theme 4: Legacy Systems and Modernization Strategies

The fourth cluster addresses the complex and persistent role of legacy systems in financial IT infrastructures. They are no longer seen as mere technological artifacts of the past; legacy systems were described as deeply embedded components of organizational knowledge, operational stability and business continuity. In many cases, they continue to support core business processes.

Respondents repeatedly challenged simplistic definitions of legacy. Many interviewees emphasized that these systems are not inherently obsolete but are evaluated in terms of functional adequacy and contextual relevance (K11, K26, K71). Despite their technical debt, their perceived value is often indispensable; legacy systems exhibit strong stability and performance, particularly in mission-critical environments. Thus, institutional memory, risk aversion, and the cost-benefit analysis of replacement vs. retention are all factors in the legacy discourse.

Nevertheless, modernization remains a recurring objective of complex systems, driven by dependencies across vendors and architectures, as well as maintenance challenges and integration difficulties. Participants described their modernization approaches and strategies for their legacy systems ranging from incremental modularization (K73) and controlled parallelization (K57, K72) to compatibility-driven interface redesigns (K41). The understanding that “big bang” migrations are rarely possible, but sometimes inevitable in highly regulated and networked environments, is reflected in these methods.

Conflicting stakeholder interest are further complicating strategic decision-making regarding modernization. The interplay between internal actors (e.g. operations, risk, development), external service providers and product vendors (K12) often arise tensions, particularly when legacy systems represent a revenue stream or risk exposure. In this situation, legacy modernization becomes a political and economic negotiation, in addition to a technical one. Nevertheless, the DevOps approach is at least one promising way to ease the conflicting tensions between developers and operations (K3, K49).

Moreover, several specialists noted that legacy architectures have evolved over time, giving rise to hybrid systems that combine modular or API-based frontends with monolithic

cores (K73). This “dual-mode IT” allows for some degree of agility while preserving core stability—a compromise shaped by continuous organizational learning.

In summary, legacy systems extend beyond remnants of outdated technology but are active components of complex socio-technical systems. Their role is best understood through a lens of strategic value, path dependency, and pragmatic modernization. Successful transformation requires nuanced, context-aware strategies that balance risk, cost, and architectural evolution while maintaining a holistic view of the overall system.

### 7.3.5 Theme 5: Performance Metrics and Experience Blind Spots

This thematic cluster highlights the tension between metric-based governance and experiential service realities in complex IT systems. Across interviews, metrics were found to be essential steering instruments, but the actual implementation of them was often criticized for misalignment with lived service quality.

A core insight is the disconnect between user-centric performance and technical KPIs (K35, K48). As an example, an availability metric may report “green” service states, even though the user experiences delays, inconsistencies, or degraded functions. False-positive indicators were noted by multiple participants and seen as a key challenge for meaningful evaluating services.

Furthermore, simplicity and aggregability are managerial demands which can lead to the oversimplification of complex service behaviors. These metrics are depicted in dashboards, traffic-light systems, or single-value indicators (K9), which can obscure important details. The nuanced system states are lost during translation and misinterpretation, increasing pressure on operational teams.

To mitigate this, the organizations are resorting to experience-based or qualitative feedback loops (K19, K33). These can come in different forms — supplier evaluations, retrospectives, consultations, and workshop-based satisfaction scoring. Despite providing greater context, these techniques are generally non-standardized and more difficult to institutionalize.

Several participants noted that they have made efforts to close the gap between evaluations and efforts, via trend-based and role-specific KPI monitoring (K52), as well as conducting structured lessons learned sessions after major incidents (K51, K66). These practices serve as a corrective measure to abstract metrics by reintroducing non-technical metrics in the form of narratives, causalities, and socio-technical interpretations into the performance evaluation.

Importantly, these insights suggest that mere quantitative metrics are insufficient to fully illustrate service health. Metrics provide orientation and are often good indicators, but have to be complemented by contextualized and triangulated sources, methods or perspectives. Nonetheless, the expertise of contributors should challenge metrics with iterative feedback and stakeholder engagement; otherwise, the risk of blind spots exists.

### 7.3.6 Theme 6: Governance Models and Change Management

This theme centers on the institutionalization of formal control systems in IT service environments through clearly defined governance frameworks and change management practices. The interviews revealed a clear reliance on formalized frameworks for ITSM. ITIL, CABS, KPI hierarchies, and service maturity models are examples of tools used to standardize decision-making and ensure process stability (K17, K32, K42, K58, K59).

Participants characterized governance models as an essential support structure for disciplining operations, enforcing accountability, and managing risks in highly regulated and distributed environments. Good examples are change processes, which are structured via tiered approval workflows and impact-based classification. All of this is aimed at mitigating service disruptions and maintaining auditability (K42, K58).

Conversely, these structures also reveal frictions. Process overhead and documentation requirements are a burden for workers, particularly those involved in time-sensitive or agile development contexts (K29). Cultural inertia and communication barriers were stated as additional factors for impediments to effective implementation, leading to delays, ambiguity, or misaligned expectations across teams (K28, K30, K61).

Global standardization efforts, whether from standardization institutions or holding structures, were seen as a double-edged sword (K63, K74). Despite their promises of efficiency and coherence, globalization frequently leads to longer lead times for even small system modifications and a loss of local autonomy. Lastly, they also increase the coordination load, with higher documentation costs and more complex accountability structures.

Respondents also described tooling strategies and modifiability trade-offs (K60), where governance is embedded into service platforms like ServiceNow. Similar patterns appear with frameworks, where dependencies on frameworks such as ISO/IEC 20000 bring similar effects. These implementations facilitate standardization, but also bring new complexity drivers, especially if over-customized or insufficiently aligned with actual practices.

Governance was described as a cultural construct of the institutions rather than just a formal structure. Effective change management was enabled by a successful integration of leadership commitment, with good communication strategies that provide a gradual cultural adaptation. This can be reinforced by training, gamification and true value-based messaging to all stakeholders (K12, K59, K61).

This theme highlights the ongoing interplay between flexibility and formal control. While governance frameworks and specific tools provide essential structure, they must be adapted in implementation to a degree that allows them to be culturally internalized in order to remain effective.

### 7.3.7 Theme 7: Regulatory Demands and Compliance Automation

This theme addresses the growing influence of regulatory mandates on the design, execution, and evolution of service management in the financial IT domain. Regulatory

frameworks are versatile and expanding with GDPR, DORA, Solvency II, MiFID II, and Payment Card Industry Data Security Standard (PCI DSS) all mentioned throughout the interviews. These regulations are not only compliance obligations but also strategic determinants of service architecture, procedural priorities, and risk management philosophies (K17, K47, K50).

Interviewees consistently described regulatory complexity as a structural force that both shapes and constrains operational flexibility. Release schedules, system design decisions, and documentation procedures were observed to be dictated by compliance requirements. Entire governance models were framed around auditability, often to the detriment of agility or innovation (K75).

One trend observed was the delegation of compliance responsibilities to third parties (K38), particularly in outsourced service environments or cloud-based systems. This can reduce internal workload but also introduce new dependencies and additional complexities. External certifications, such as ISO/IEC 27001 or System and Organization Controls 2 (SOC2) reports, are required, as well as a general trust in partners and their audits, often without granular visibility or automated control mechanisms.

RegTech and compliance automation are measures used to respond to these challenges (K10, K56, K70). Participants mentioned automated policy checks and structured incident escalation based on regulatory thresholds. Artifact mappings were also described, where artifacts produced by the system are mapped directly to regulatory requirements. However, completely automated regulatory compliance is not feasible, since technical support is limited to procedural initiation or evidence collection, with legal interpretation and strategic responses still relying on human oversight.

The tension between automation and explainability is further complicates this effort (K10, K79). As systems become more autonomous, especially when AI is involved and the trend is going in this direction, organizations face difficulties justifying algorithmic outcomes to auditors or regulators. This leads to a dilemma in which automation can speed up the supply of compliance but may compromise interpretability and transparency.

Actual system hardening or operational resilience is often neglected due to significant effort in fulfilling compliance documentation requirements. Similar to the “illusion of precision” dilemma in service metrics, the resource allocation dilemma of hardening the system and documenting completed work reflects this tension. Addressing this challenge will require more integrated and context-aware compliance mechanisms in the future.

Overall, this theme illustrates that regulation provides structure and cannot only be seen as a complexity driver or constraint for organizations. Often, regulations depict that great work has been done and that the systems are compliant with a particular standard, provided documentation overhead remains manageable. Navigating this needs technical automation and institutional alignment, as well as a design for auditable systems.

### 7.3.8 Theme 8: Adaptive Steering and Predictive Capabilities

The final theme captures a future-oriented dimension of service management in complex IT systems. As complexity rises, interviewees highlighted the growing importance of dynamic steering mechanisms beyond static planning.

Unpredictability was a recurring pattern and a fundamental condition in complex systems (K15). Service management with predefined responses is increasingly outpaced by emergent issues. As a result, organizations are shifting from rigid planning to situational response models. This shift is reinforced by PIR routines, which revise processes with lessons learned and causal probability mappings (K20, K66).

High maturity organizations are attempting to address volatility through predictive maintenance and resource forecasting based on historical usage patterns (K54). While this is a promising approach in theory, they are often constrained to a small, isolated part of a system. Data limitations, architectural fragmentation, and the challenge of generalizing predictive models to non-deterministic systems remain significant obstacles (K78).

Asset management was also mentioned as an underestimated factor. Asset management, encompassing all tangible and intangible assets, especially within SIAM environments, is essential for adaptive management yet often lacking in quality and completeness. Efforts like predictive maintenance and adaptive service management remain disjointed and prone to errors without trustworthy asset data (K77).

Flexible resource allocation and emergency capacity planning are needed for strategic adaptability. These measures support unplanned work or enable adjustable project portfolios (K44). Resource pooling or bench management is a tactic to allocate the right amount of resources when needed. These mechanisms reduce project derailments in highly dynamic vendor ecosystems.

Another key component is to integrate service management into different frameworks, such as security and risk (K79). A holistic system overview combines operational, compliance, and risk indicators into coherent dashboards. Nonetheless, this task remains under development in most cases.

Finally, this cluster includes reflections on strategic alignment between IT operations and business goals (K34, K49). The trade-offs between multiple actors, such as speed, quality, and risk, must be constantly recalibrated under changing conditions. To adapt to system states, the priorities must be evaluated.

In summary, this topic demonstrates that strategic adaptation in complex IT systems involves planning for unpredictability more than predictions. Modular governance structures, reflexive learning cultures, and the ability to synthesize fragmented signals into coherent decisions are strategies for enhancing adaptive capabilities.

# Discussion

## 8.1 Introduction

This chapter discusses the empirical findings from the expert interviews in relation to the previously defined RQs, hypotheses, and the theoretical background presented in Chapters 4 to 7. The structure follows the core RQs, and within each section, the relevant hypotheses (H1–H5) are critically assessed, along with their comparison to the literature and the overall implications.

## 8.2 RQ1: How do businesses in the financial sector measure the success of service management practices in complex IT systems, and what metrics or indicators are used?

### Related Hypothesis

H1: In complex financial IT systems, the incorporation of continuous improvement metrics (e.g., frequency of PIRs, learning velocity) and experience-based metrics (e.g. XLAs, customer satisfaction), in addition to traditional technical metrics (e.g. uptime, MTTR), provides a more holistic measure of service performance than relying solely on technical indicators.

### Summary of Interview Findings

The results reveal that organizations in the financial sector are understanding service performance increasingly differentiated. Traditional metrics, such as indicators of uptime, availability, MTTR, response time, etc. (K65, K48) remain important as a reporting structure. However, in cases where aggregated values distort the results, these metrics

## 8.2. RQ1: How do businesses in the financial sector measure the success of service management practices in complex IT systems, and what metrics or indicators are used?

---

reach their limits (K9, K35). Therefore, relying solely on technical metrics fails to accurately reflect user experience.

Instead, qualitative and experiential metrics are integrated by the respondents. Some examples for subjective evaluations are supplier feedback, retrospectives, user interviews, or lessons learned cycles. These provide the service quality view from a user's perspective (K19, K33, K66). Furthermore, continuous improvement metrics and a culture which strives for this are evident to help improve service metrics. Measures to help improve service metrics could include PIRs or operational handover practices (K51).

Next, there are accountabilities at the process level; each process should have an accountable person and a meaningful metric, otherwise the process is obsolete. Therefore, KPI ownership can optimize this setting; the owner is better able to detect trends, identify outliers, and improve this process continuously. Nonetheless, the metric landscape often remains incomplete (K4), which impedes systematic evaluation of side effects and emergent behavior (K35, K37).

The approach to managing this demand is to combine technical indicators with experiential indicators. RCA, incident classification, and process metrics such as time-to-resolution showcase this combined approach (K48, K65). In some cases, predictive maintenance techniques and historical pattern analysis are applied, although typically in isolated system segments (K54, K78).

### Comparison with Literature

Recent literature predominantly questions traditional service metrics. Although these metrics remain central to established frameworks like ITIL and COBIT [9, 58], their ability to truly reflect operational reality in complex IT systems is limited. This critique is consistent with the interviews, where quantitative metrics can obscure disruptions and degrade the accuracy of user experience assessments [96, 21].

An underlying problem is the mismatch between static, aggregated indicators and the dynamic, emergent nature of complex systems. Scholars such as Mitchell and Toroczka [80], Lindgren [66], and Tranquillo [111] argue that non-linear feedback, dependencies, and the systemic uncertainty shape service outcomes. The respondents' suspicion of over-aggregation and indicator abstraction reflects the possibility that isolated KPIs may miss cross-domain effects or hidden weaknesses (K9, K35).

The literature highlights the relevance of experience-based metrics to complement technical indicators. Often formalized as XLAs, these metrics have gained traction in the academic and professional discourse [70, 19]. Interviewees reported a growing role for these qualitative feedback metrics, though they are often applied informally. The scope of XLAs is seen as limited, particularly since the actual consequences are not always clear. The rationale aligns with the service-dominant logic [113], in which the perceived value and co-created outcome are effective measures to evaluate service effectiveness.

## 8.2. RQ1: How do businesses in the financial sector measure the success of service management practices in complex IT systems, and what metrics or indicators are used?

---

Further agreement across sources is found in continuous improvement [40, 26]. Multiple patterns were found that prove that embedded learning with feedback loops (K51) contributes to metric development, but also improves the overall maturity of processes.

While the literature on governance often states role clarity [17, 58], it rarely addresses the impact of individual KPI ownership. Participants have mentioned this as a decisive element in improving metrics and interpreting trends (K52). Therefore, a conceptual gap between formal governance models and real-world service oversight could be observed.

Structural limitations of service metrics were also noted in both domains. Alt, Beck, and Smits [3] and Puschmann [91] discuss architectural fragmentation and legacy constraints in many financial IT systems. Interviews confirmed that metric systems complicate the detection of emergent behavior (K4, K37). In particular, siloed measurements lack systemic visibility [67].

The literature reflects broader findings, cautioning against overestimating the maturity of predictive systems in heterogeneous, loosely coupled IT environments. Despite extensive promotion of predictive and adaptive monitoring [71, 78], there is still limited practical application of these techniques. Persistent challenges in architectural mapping and data integration (K67) confirm this, specifically in systems that use predictive maintenance and anomaly detection (K54, K78).

### Interpretation and Hypothesis Evaluation

H1 is strongly supported by these findings. Technical indicators alone are insufficient for evaluating service performance in complex environments accurately. A shift occurred, integrating multidimensional metrics from socio-technical and experiential evidence. Post mortems and qualitative feedback emerge as essential practices of continuous improvement (K19, K51, K66), validating the hypothesis.

### Implications

The evaluation of service performance in complex IT systems for the financial sector demands a multidimensional measurement logic, which reflect both operational behavior and user experience. To achieve this, organizations should integrate feedback loops and continuous improvement routines in their measurements. Moreover, assigning ownership to KPIs enhances metric interpretability and drives adaptive responses. More accurate evaluations of service quality in dynamic situations are made possible by a metric landscape that is cohesive and well-managed.

## 8.3 RQ2: How do stakeholders in financial institutions evaluate the effectiveness of service management metrics in complex IT environments?

### Related Hypotheses

H2: Multi-layered monitoring (e.g. real-time telemetry, role-based dashboards, event-driven alerts) proves as more effective in capturing the full spectrum of service performance. This leads to stakeholders evaluating these metrics more favorably than static or siloed approaches in the service management of complex IT environments in the financial sector.

### Summary of Interview Findings

Stakeholders in the financial sector assess service management metrics based on their ability to represent the operational reality of their complex systems. A preference towards multi-layered monitoring, along with strategies to adapt monitoring practices to environmental conditions, has been identified. This is established through role-specific dashboards based on individual specifications and real-time telemetry. Together with alert-driven logic, these approaches provide greater transparency and more effective controls in the dynamic service landscape (K21, K22, K36).

The central benefit of multi-layered monitoring is its ability to integrate data from different sources and consolidate it in one place. This allows to detect irregularities as soon as data is updated (K21, K36, K67). Several interviewees described their setups as more responsive and reliable when using this approach. This also allowed for faster incident detection and escalation paths, especially in high-frequency chains of system components (K36).

Key challenges that still exist are fragmented toolsets, which create gaps in system-wide visibility (K6, K4, K37). The limiting factors are monitoring systems that depict isolated metrics without sufficient contextual aggregation across services and their boundaries; this limits their usefulness (K4, K35, K37).

Organizations with high log maturity adopt adaptive monitoring strategies, in which log depth can be dynamically adjusted based on the environment (K68). Stakeholders can analyze pertinent patterns more freely in these setups without being overburdened by noise or overhead. These practices are seen as superior to fixed monitoring templates and are viewed favorably, especially when services are aligned with business processes (K22, K68).

Moreover, to track emerging deviations and support informed decision-making, stakeholders implemented KPI ownership with additional cross-functional visibility (K52, K67). Interviewees did, however, highlight the difficulty in evaluating aggregated indicators, which can obscure localized problems and create the false impression of control (K9, K35, K66).

### 8.3. RQ2: How do stakeholders in financial institutions evaluate the effectiveness of service management metrics in complex IT environments?

---

#### Comparison with Literature

Mittal, Diallo, and Tolk [81] and Tranquillo [111] recognized that volatile environments require metrics that are interpretable and context-aware within the ecosystem. In addition, these metrics should be integrated into the operational workflows. This finding has also been found in the interviews, which indicated that metrics should be responsive to system dynamics, frequently shifting from conventional performance reporting.

A key area of alignment is the findings on multi-layered monitoring. Modern monitoring architectures combine data across multiple layers, often visualized through role-specific dashboards [71, 78]. This also reflects the reported interviews, where cross-layer visibility was deemed necessary (K21, K36, K67).

Building on this, notions that define observability not simply as availability, but as the ability to expose internal states in an understandable way have emerged [66, 21]. The operationalization of this idea is shown in the adaptive monitoring techniques identified in the interviews, such as contextual escalation or variable log depth (K68). SRE models, which advocate for observability as a governance tool to manage uncertainty, are consistent with these methods [70].

Yet this monitoring approach has constraints; the data highlighted gaps in systemic traceability caused by missing context within monitoring tools (K4, K6, K37). This is also documented in the literature on legacy architectures and additional vendor-induced complexity [3, 60]. Without consistent architectural mapping, even well-designed indicators lose their evidential value.

A concern in the literature and the interviews is the loss of granularity through aggregation. While aggregated metrics can offer summaries and show emerging behavior, they can also conceal localized failures (K9, K35, K66). Mitchell and Toroczka [80] and Liu and Barabási [67] also stress that simplified indicators obscure the volatile nature of interconnected systems. Therefore, the interpretive alignment of a metric with the stakeholder's context is more important than its quantitative accuracy.

Accountability in metric interpretation is not only a governance measure, but a way to enable responsive trend detection and corrective action (K52, K67). This finding complements research, which states that indicators gain significance when they are operationally anchored and interpreted locally [17, 111].

The effectiveness of metrics improves when they are aligned with business processes. Interviewees described this in terms of adaptive monitoring designs that respond to the criticality and context of services (K22, K68). This is echoed by literature emphasizing that static metrics across heterogeneous services limit strategic oversight [71, 19].

Finally, the signal-to-noise challenge in log-data is a shared concern, as high volumes can overwhelm human interpretation unless pre-filtered. Selective log activation and dynamic scoping are responses to this oversaturation (K68); these approaches mirror discussions on metric fatigue and observability debt [96, 78].

#### 8.4. RQ3: What role do automation and monitoring tools play in managing service delivery in complex IT systems, and to what extent are their benefits and limitations observed?

---

### Interpretation and Hypothesis Evaluation

H2 is supported by these findings. The empirical evidence consistently reports multi-layered monitoring and contextualization to be more effective in complex service environments. By offering a granular and responsive approach configurable for individual roles, such systems allow stakeholders to make more informed and actionable decisions. The need for dynamic, role-oriented settings is further supported by the drawbacks of isolated and static monitoring, which frequently produce blind spots or aggregated distortions.

### Implications

Effective service evaluation in financial institutions with complex IT environments requires monitoring systems that are context-sensitive, role-specific, and, when necessary, dynamically adjustable. The most beneficial are multi-layered systems that align with business processes and operational workflows. Static or siloed monitoring, by contrast, obscures critical deviations. Therefore, to provide real-time evaluation and well-informed intervention across service borders, organizations should prioritize integrated monitoring systems with adaptive depth and clear KPI ownership.

## 8.4 RQ3: What role do automation and monitoring tools play in managing service delivery in complex IT systems, and to what extent are their benefits and limitations observed?

### Related Hypotheses

H3: In non-deterministic complex IT systems in the financial sector, where behavior cannot be fully predicted or reproduced, adaptive monitoring and quality assurance practices (e.g., dynamic SLOs, anomaly detection, resilience engineering) are more successful in maintaining service quality and operational control than those relying on deterministic models. H4: In the service management of complex financial IT systems, automation and monitoring tools that embed security and compliance checks (e.g., ‘policy as code,’ automated compliance gates) significantly enhance release velocity and reduce risks.

### Summary of Interview Findings

The interviews showed that automation and monitoring tools are central enablers of service delivery in complex financial IT systems. Their effectiveness depends on the integration and adaptability of the implemented solutions.

Regarding adaptive monitoring and quality assurance, stakeholders noted that traditional metrics fall short in dynamic environments (K15, K35, K37). Instead, new solutions emerged, which provide anomaly detection and service behavior analysis, such as User and

#### 8.4. RQ3: What role do automation and monitoring tools play in managing service delivery in complex IT systems, and to what extent are their benefits and limitations observed?

---

Entity behavior Analytics (UEBA) (K22, K36, K67). This provides better control over unpredictable behaviors, particularly in critical systems. Further, adaptive monitoring supports faster fault isolation and escalation, allowing service teams to respond to emergent phenomena (K36, K68).

The limits of deterministic models universally acknowledged by the respondents. It is impossible to plan for all failure modes in interconnected systems (K15, K62). Therefore, resilience engineering practices and layered telemetry should be practiced (K21, K22, K44).

In terms of automation, several patterns emerged regarding the impact of service quality and speed. In the development phase, stakeholders reported a fast deployment velocity and higher confidence in operational integrity. To accomplish this, automation pipelines were implemented, including embedded security and compliance checkpoints with digital sign-off procedures (K23, K70, K56). This benefit was especially prevalent in regulated environments, where audit trails are necessary (K10, K17, K23).

However, the limitations of full automation were also recorded. The importance of fallback mechanisms has been stressed, as well as manual overrides or four-eyes principles, especially for high-risk operations (K24). Furthermore, false-positive alerts and uncontrolled automation behaviors introduce new risks. This leads to a need for architectural maturity and monitoring clarity that supports automation (K53, K69).

Overall, the benefits of automation and monitoring stem from co-evolution, where tooling is integrated into a layer of governance and observability. The combination of policy-aware deployment, adaptive alerting, and service-aware architecture maps (K21, K22, K53, K79) reflects the direction of more mature organizations.

### Comparison with Literature

In both academic discourse and empirical findings, automation and monitoring have shifted from isolated features to core processes [71, 111]. Rather than being technical implementations alone, they evolved into socio-technical infrastructures.

Monitoring has shifted from static reports to dynamic capabilities, embedded in system architectures. Participants showed that organizations are adopting behavior-based detection and adaptive telemetry (K22, K36, K67), reflecting literature that emphasizes observability as essential [70, 21]. Deterministic monitoring has more limitations; for example, when defining thresholds (K15, K35, K68), this reinforces calls for adaptive monitoring [67, 66]. Monitoring is also described as a detective measure for increased responsiveness, rather than a tool for certainty [111, 81].

The role of automation remains ambivalent, although widely endorsed. On the one hand, automation enables velocity and assurance (K23, K70), but on the other hand, new risks emerge from insufficient oversight (K24, K69). This is also found in literature, where automation can introduce new complexity if not grounded in traceability and governance [3, 6].

#### 8.4. RQ3: What role do automation and monitoring tools play in managing service delivery in complex IT systems, and to what extent are their benefits and limitations observed?

---

Crucially, automation's effectiveness depends on clear dependencies and boundaries [71, 60]. This is substantiated by findings that describe an accompanying process which provides control and oversight over automation (K24, K56, K70). However, some concepts, such as policy as code, remain unsupported in practical settings (K10, K17, K23).

Architectural maturity is closely tied to the effectiveness of automation; clear benefits arise when automation is grounded in clear service mappings and cohesive system structures (K53, K79). Puschmann [91] and Alt, Beck, and Smits [3] also argue that automation deployment should be cautious in fragmented environments. In incident management, reactive and proactive automation strategies are both applied, yet interpretability and control must be given. This is written in the literature, highlighting that responsiveness and oversight have to be balanced [18, 1, 97], and revealing a gap in understanding how automation can be governed effectively in complex settings.

### Interpretation and Hypothesis Evaluation

H3 is strongly supported by these findings. Statements consistently prove the need for real-time, dynamic, and behavior-aware monitoring frameworks. Classic models, which are solely driven by SLAs, were described as insufficient in managing emergent service disruptions. Adaptive practices were viewed as more effective and aligned with system realities (K22, K67, K68, K44).

H4 is also supported by these findings. According to interviewees, compliance-integrated automation makes deployments safer, quicker, and audit-compliant, especially when it is in line with frameworks like ISO/IEC or DORA (K10, K17, K23, K56, K70). However, over-automation has been cautioned against, so a balance between the trust in automation and human oversight has to be established, with consideration of a cost-benefit analysis (K24, K25, K69).

### Implications

In complex IT systems, automation and monitoring must be treated as interdependent tools rather than isolated technical features. Adaptive monitoring enables responsiveness to emergent conditions, while automation enables speed and consistency, provided that control structures and boundaries are in place. Safeguards, including fallback mechanisms, should be implemented. To fully utilize automation in service delivery, institutions should match tooling to architectural maturity and regulatory requirements.

8.5. RQ4: What specific service management strategies are adapted by businesses in the financial sector to handle the increasing complexity and interdependencies of modern IT systems?

## **8.5 RQ4: What specific service management strategies are adapted by businesses in the financial sector to handle the increasing complexity and interdependencies of modern IT systems?**

### **Related Hypotheses**

H5: Financial institutions that approach legacy-system modernization as a continuous, feedback-driven strategy, rather than one-time transformations, achieve more robust service management outcomes and reduce technical debt over the long-term on highly complex IT systems.

### **Summary of Interview Findings**

The interviews demonstrated that dealing with complexity in financial IT systems requires continuous, feedback-driven strategies embedded in organizational routines. In particular, change management and transformation projects should constitute an ongoing, iterative process (K11, K57, K58).

Respondents described multiple modernization approaches, notably dual-platform strategies, which allow for old and new components to coexist, as long as they are not End of Life (EoL) (K26, K41, K57). This logic reflects that legacy systems are not only a source of technical debt but also a critical stability anchor in production (K26, K71).

Furthermore, legacy systems are rarely seen as obsolete in terms of functionality. Rather, they constitute infrastructures with a purpose embedded into the complex environment of different stakeholders and regulations (K11, K46, K47). Modernization is therefore a politically charged process that necessitates cooperation, negotiation, and approval among departments and suppliers (K12, K45, K29).

Importantly, feedback mechanisms such as lessons learned, incident reviews, and structured handover practices were frequently mentioned as essential parts of this transformation strategy (K19, K51, K66). This helps to recognize parts of the system which need to be changed, replaced or phased out. Technical debt can be controlled, and newer solutions enabled over time (K72, K58, K66).

Service management can also benefit from governance-based change control and a culture that promotes improvements (K58, K59, K61). Moreover, the value of legacy systems is often reevaluated with respect to business alignment and service continuity, rather than architectural purity (K30, K57, K72).

In addition to legacy management, other strategies were employed to handle architectural and operational interdependencies. Efforts to build SOA, which break down isolated silos and reduce coupling, were undertaken (K64, K73). However, this design change also led to unintended complexities. Examples for side effects arising from a modular design

## 8.5. RQ4: What specific service management strategies are adapted by businesses in the financial sector to handle the increasing complexity and interdependencies of modern IT systems?

include microservices sprawl or decoupled monoliths, which are interface dependency proliferations (K8, K73).

To combat this, adaptive monitoring architectures with dynamic and multi-layer observation capabilities were implemented (K21, K67). This is supported by anomaly detection and context-specific alerts, which offer better visibility and control in complex environments (K22, K36, K68).

Another strategy focuses on the organizational structure, cross-functional service teams (e.g. DevOps), and role integration across IT and business domains, which aim to reduce friction in operational coordination and increase ownership at the service level (K28, K30, K18). This team structure offers more reliable and efficient service delivery, even in crisis situations.

Further, organizations mentioned strategic asset management as an effective service management tool. As complexity increases through outsourcing and heterogeneous platforms (K77), the overview deteriorates. Therefore, good data quality in SIAM platforms was seen as essential.

Finally, service management was structured using regulatory and governance frameworks (such as ITIL, DORA, and ISO/IEC), although not always in ways that were compatible with agile methods (K17, K32). This led to compliance automation where possible and to growing interest in lightweight control loops for faster response and a reduction in audit overhead (K70, K56, K44).

### Comparison with Literature

Managing complex IT systems in the financial sector requires service management strategies that are adaptive and promote continuous learning, as depicted in empirical data and literature, which also state limitations of linear approaches [111, 109].

Complexity theory and interviews indicate that continuous change is, in most cases, better than isolated transformation projects (K11, K57, K58) [80, 66]. Change management in this situation shifts constant recalibration in light of changing system conditions. In previous research, legacy systems were frequently viewed as liabilities [3, 91]. However, they are now acknowledged as essential infrastructures that support business logic and regulatory continuity [71]. The participants stated that legacy systems are often a stabilizing factor (K26, K41, K71), allowing for gradual modernization [96, 60]. Such transitions require consistent governance, as challenges exist in coordinating stakeholder groups and managing political frictions (K12, K45). Literature on IT change confirms that complexity demands structured coordination and regulatory oversight [81, 46].

Early literature already states that learning loops that recalibrate system behavior and decision logic over time, are essential for effective processes, as noted by Eisner [40] and Braun and Clarke [26]. Such routines, which guide incremental improvements, were confirmed by interviewees (K19, K51, K66).

At the organizational level, cross-functional teams are deemed important to improve coordination across IT and business interfaces while also reducing friction (K18, K28, K30). The literature describes these benefits as including higher responsiveness and more resilience under uncertainty [70, 21].

Strategic asset management is another domain where theory and practice converge. Asset visibility and configuration integrity, long overlooked in service literature, are becoming more widely acknowledged as the cornerstones of successful orchestration (K77).

Finally, standard-based and regulatory governance remains influential. Although many frameworks exist, their integration with agile or adaptive practices is limited (K17, K32). Academic calls for compliance automation and RegTech integration as mechanisms to reduce audit overhead and increase organizational responsiveness are present [60, 78]. The interview data showed nascent implementations, but they are not as extensive as described in the literature (K70, K56, K44). This underscores the maturity gap between intent and execution.

### Interpretation and Hypothesis Evaluation

H5 is strongly supported by these findings. Financial institutions that approach legacy transformation as a long-term process report better results and resilience. The consistent emphasis on incremental integration, technical continuity, and cross-functional learning (K51, K57, K58, K66) illustrates the success of this approach in maintaining control and building more sustainable architectures.

### Implications

Many different strategies are used for service management of modern IT systems in the financial sector, and some factors should be prioritized, such as efficiency, continuity, adaptability, and cross-functional alignment. When modernizing IT systems, an ongoing process should be established to incrementally decommission legacy components while implementing new solutions, anchored by structured feedback and governance. An overview of the service structure, supported by monitoring solutions, architectural visibility, and effective asset management, is also essential. Lastly, compliance mechanisms must be implemented in ways that support daily operations and transparency to stakeholders.

## 8.6 Strengths and Research Contributions

This thesis offers a contribution to the underexplored intersection of service management and systemic complexity within the financial sector. The thematic analysis is one key strength, as it conducts expert interviews with senior practitioners from diverse financial institutions, through which practice-based insights are captured that extend beyond theoretical assumptions. As a result, a multidimensional view of complexity and its management has been established by integrating both strategic and implementation-oriented roles.

One strength is the research design, which deliberately sampled experts with substantial professional experience and deep domain expertise. Moreover, although all interviews were drawn from the financial sector, the institutions represented a wide array of organizational types. Each company operated under different regulatory logics and service delivery models. The empirical basis was enriched by this institutional diversity, which rendered the conclusions more broadly applicable.

Next, there is a strong alignment between theory and empirical investigation. Complexity is not a background condition, but a central analytical topic. The conceptual integration of complexity theory with service management enables a more realistic understanding of how emergent behavior, legacy constraints, and interdependencies shape service strategies in modern IT landscapes.

The thematic analysis provided enough flexibility to find patterns across heterogeneous data while still maintaining analytical rigor. With a two-phase interview structure and a consistent design, the findings could be better identified and applied.

Finally, the thesis contributed to the professional and academic discourse by identifying structural and practical challenges, while also providing potential solutions. This forward-looking view on service management practices allows for gain of maximum value for the audience.

## 8.7 Limitations and Critical Reflection

While the thesis provides valuable insights into service management strategies for complex IT systems in the financial sector, it is not without limitations.

First, the sample size of seven experts across six interviews is relatively small. Although sufficient for exploratory qualitative analysis, it limits the representativeness of the findings. Insights are reflected from senior-level professionals from Austrian financial institutions, and while this provides useful context on the diverse financial institutions, it may not capture the full diversity of strategies used in other geographic or regulatory environments.

Second, confirmation and response bias are possible due to participants being embedded in their own respective systems. They may base their views on institutional expectations. Moreover, the semi-structured interview format derived themes from prior hypotheses and literature. Although inductive coding was used to mitigate this, it could have limited the formation of entirely novel insights.

Third, this exclusive focus on the financial sector, which operates under strict regulations and has unique operational characteristics, limits the generalizability of the findings. Consequently, direct transferability to other industry sectors should be approached with caution.

Another important limitation concerns potential biases in the research setting, as some participants were known to the researcher through previous professional or academic

contexts. A possibility for response bias exists, where respondents may answer in a different or more favorable way. Similarly, the researcher's knowledge of the topic and interview subjects may have affected how questions were phrased or how answers were interpreted. Although anonymization, consistent interview protocols, and a reflexive approach during analysis helped reduce these risks, they cannot be completely eliminated.

Furthermore, the literature base found for this research provided its own challenges. Although many sources exist on service management, complex systems, IT governance, IT systems in the financial sector, and digital transformation exists, only a limited subset directly addresses the intersection of multiple parts with system complexity, especially within the financial sector. As a result, to draw conclusions, the literature review had to draw on adjacent disciplines and general management frameworks, leading to the extrapolation of insights to fit the research context. This broadened scope enriched the conceptual foundation and was recorded in detail, but it may also introduce interpretive risks due to differences in sectoral focus or theoretical framing.

Despite its limitations, the findings form a robust foundation for understanding how service management works effectively in complex IT systems within the financial sector. Future research might be expanded upon by using quantitative validation, cross-sector comparisons, or longitudinal studies that show how strategies change over time.

# Conclusion

This thesis presents how service management within complex IT systems in the financial sector should be practiced and which strategies are most effective. The landscape of complex environments is shaped by dynamic interactions among independent components in an infrastructure, characterized by heterogeneity and interdependence. Consequently, their behavior also becomes non-linear and unpredictable. Thus, the relevance of the topic arises from its immediate practical implications for ensuring reliable service delivery, but also from its theoretical necessity to reframe service management as a discipline capable of engaging with systemic complexity in a methodologically and conceptually robust manner.

In this context, complexity is a situation that has become essential to the functioning of vital services rather than an exception or anomaly. Therefore, the empirical findings show an increasing need for institutional adaptability. It became evident, that effective service delivery relies on the capacity of organizations, to adjust practices and incorporate system feedback in an ongoing manner. Service management cannot be understood as a standardized control function, but must be conceptualized as a dynamic and situational process that reflects evolving constraints. One of the main resources to achieve this is data which give a holistic view on services and can be used to improve and modernize processes. This information should include quantitative and qualitative metrics and be present in a meaningful observation platform. Another factor is the deployment of automation which helps manage tasks, but is structured in a way that allows for traceability, because of regulatory constraints.

The implications of the findings are significant. Service management is not only a technical function located downstream of IT development, but is increasingly seen as a core site of coordination spanning across the entire service lifecycle. It extends from development through operations, but must also account for dynamics in the system, beginning at the evolving interdependencies between components to regulatory constraints. This creates tensions between reliability and change, standardization and innovation, or internal

---

policies and external expectations, all of which have to be managed. Institutions that find a balance between these tensions and treat service management as a continuous process of learning are able to reach higher service management maturity and better performance in service delivery and resilience.

This thesis contributes to the academic discourse by addressing a notable gap in the intersection of complexity theory and ITSM. While complexity is often seen as a buzzword or marketing term, it is rarely attested with foundational literature. The literature itself has long acknowledged the relevance of systemic uncertainty and interdependence in large-scale IT systems, but few empirical studies have applied these concrete practices to service management, particularly in highly regulated sectors such as finance. This research provides an empirically supported explanation of how institutions modify their strategies in the face of complexity by fusing theoretical viewpoints on complexity with qualitative insights from expert interviews. Through the qualitative approach, situational perspectives with practical insights could be captured. In doing so, the thesis establishes a valuable foundation for further investigation into the institutional capacities and epistemic practices that underpin service management in complex IT environments.

Future research may extend the investigation through complementary perspectives. Quantitative studies could further assess the impact of the identified themes and implications by broadening the empirical base. Cross-sectoral comparisons could reveal whether the patterns seen are unique to the finance industry or suggest a more general transformation in service management. Longitudinal research may further explain how organizations are internalizing feedback mechanisms over time and whether adaptive practices are becoming more structurally embedded or remain contingent on individual actors and components. Such investigations would deepen our comprehension of the practical governance of complex IT systems and aid in the creation of frameworks that consider institutional heterogeneity and systemic realities.

# Acronyms

- ABAC** Attribute-Based Access Control. 49
- ABM** Agent-Based Model. 13, 16
- AI** Artificial Intelligence. 27–43, 49, 56, 71–73, 76, 97, 98
- AIOps** Artificial Intelligence for IT Operations. 34, 37, 43, 53, 54, 64, 72
- BCM** Business Continuity Management. 35, 41
- BRM** Business Relationship Manager. 51
- CAB** Change Advisory Board. 47, 52, 75, 98
- CAS** Complex Adaptive Systems. 23, 46, 49, 55, 56, 60, 61
- CCPA** California Consumer Privacy Act. 40
- CI/CD** Continuous Integration / Continuous Delivery. 36, 50, 98
- CIA** Confidentiality, Integrity, Availability. 33
- CIF** Critical or Important Function. 48
- CISO** Chief Information Security Officer. 68
- CMDB** Configuration Management Database. 62
- COBIT** Control Objectives for Information and Related Technologies. 34, 35, 38, 42, 79
- Cod** Cost of Delay. 57
- CSP** Cloud Service Provider. 40
- DevOps** Development and Operations. 36, 47, 50, 59, 65, 70, 72, 73, 87, 98, 99
- DevSecOps** Development, Security, and Operations. 36, 37

- DORA** Digital Operational Resilience Act. 27, 39, 46, 48, 49, 60, 62, 76, 85, 87, 98
- DR** Disaster Recovery. 40, 41, 59
- EoL** End of Life. 86
- FinTech** Financial Technology. 5, 6, 27, 29, 32, 39, 45
- GDPR** General Data Protection Regulation. 27, 31, 33, 36, 39, 40, 49, 62, 76, 98
- GRC** Governance, Risk, and Compliance. 51, 52
- HDFS** Hadoop Distributed File System. 33
- HFT** High-Frequency Trading. 29, 30, 33, 34, 39
- IaC** Infrastructure as Code. 36, 50, 54
- IAM** Identity and Access Management. 33, 49, 50, 62
- InsurTech** Insurance Technology. 29
- IT** Information Technology. iii, 1–6, 9–18, 20–24, 27–54, 56–68, 70–75, 77–81, 83, 85–92, 97, 98
- ITIL** Information Technology Infrastructure Library. 34, 35, 38, 42, 45, 51, 52, 66, 75, 79, 87, 98
- ITSM** IT Service Management. iii, 5, 27, 28, 31, 34–38, 41–43, 45–49, 52, 53, 55–57, 59, 61–64, 67, 75, 92, 98, 99
- KCS** Knowledge-Centered Support. 56
- KPI** Key Performance Indicator. iii, 47, 60, 62, 63, 71, 74, 75, 79–81, 83, 97, 99
- LSI** Lead Service Integrator. 55
- MiFID II** Markets in Financial Instruments Directive II. 39, 46, 62, 76
- MTTR** Mean Time to Repair. 54, 59, 60, 65, 78
- NoSQL** Not only SQL. 33
- NPS** Net Promoter Score. 60
- OLA** Operational Level Agreement. 48

- PAM** Privileged Access Management. 49
- PCI DSS** Payment Card Industry Data Security Standard. 76
- PEST** Peer Esteem Snowballing. 8, 9
- PID** Proportional-Integral-Derivative. 23
- PIR** Post-Incident Review. 53, 56, 58, 65, 77–79
- PSD2** Revised Payment Services Directive. 27, 31, 33, 36, 39, 49, 62
- RACI** Responsible, Accountable, Consulted, Informed. 48, 51
- RBAC** Role-based access control. 49
- RCA** Root Cause Analysis. 36, 52, 54, 58, 79
- RegTech** Regulatory Technology. 29, 34, 36, 40, 43, 68, 76, 88, 99
- RPA** Robotic Process Automation. 58
- RQ** Research Question. 2, 4, 5, 8, 64, 78
- SaaS** Software as a Service. 97
- SD-WAN** Software-Defined Wide Area Network. 32
- SIAM** Service Integration and Management. 48, 55, 77, 87, 100
- SIEM** Security Information and Event Management. 33
- SLA** Service-Level Agreement. 35, 38, 48, 53, 54, 59, 60, 85
- SLI** Service Level Indicator. 61
- SLO** Service Level Objective. 55, 59, 65, 83
- SOA** Service-Oriented Architecture. 27, 86
- SOAP** Service Orchestration and Automation Platform. 52
- SOAR** Security Orchestration, Automation, and Response. 37, 72
- SOC** Security Operations Center. 33, 54, 71
- SOC2** System and Organization Controls 2. 76
- SoD** Segregation of Duties. 47, 49, 50
- SRE** Site Reliability Engineering. 47, 50, 55, 59, 65, 82

**SvRE** Service Reliability Engineering. 55

**SWIFT** Society for Worldwide Interbank Financial Telecommunication. 46

**UEBA** User and Entity behavior Analytics. 83

**VSM** Viable System Model. 22

**XLA** eXperience Level Agreement. 60, 61, 65, 78, 79

## Appendix A: Key Statements Overview

Code	Statement Summary
K1	Technological diversity and legacy systems contribute to technological complexity.
K2	Complexity stems from dispersed know-how, conflicting goals, and regulatory pressure.
K3	Governance is challenged by limited agility and conflicting priorities between operations and development.
K4	Metrics are fragmented and fail to reflect side effects or systemic insights.
K5	Customer-centered testing exists but lacks consistency across the system.
K6	Monitoring is fragmented with no end-to-end view of interdependencies.
K7	Automation brings standardization but also reduces flexibility and increases maintenance needs.
K8	Microservices cause unintended coupling and scaling issues despite aiming for modularity.
K9	KPIs often oversimplify and distort performance realities, driven by management desires.
K10	Compliance automation remains underdeveloped; Policy as Code is not yet established.
K11	Legacy systems are multifaceted and hard to replace, often undergoing fragmented transitions.
K12	Internal and external actors often pursue different modernization goals.
K13	AI reduces control and explainability in decision-making.
K14	AI is used to detect anomalies; Software as a Service (SaaS) products are increasingly commoditized.
K15	Complexity is marked by emergence and lack of predictability.
K16	Complexity increases when IT plays both provider and client roles.
K17	Governance is heavily shaped by regulatory standards and audits.
K18	Multiple roles and layered responsibilities challenge governance.
K19	Evaluations often rely on tacit knowledge and past experience.
K20	Incident handling involves structured cascade analysis and post-mortems.
K21	Multi-layered dashboards with role-based customization enhance monitoring.
K22	Anomaly detection and real-time performance monitoring improve security and availability.
K23	Deployment pipelines include tests, signing, and partial policy enforcement.

K24	Manual control points complement automated processes to ensure safety.
K25	Humans remain the fallback decision-makers to counter over-automation.
K26	Legacy systems persist due to compatibility and stability advantages.
K27	AI, cloud, regulation, and explainability are competing forces in tech trends.
K28	Cross-functional service teams and clear responsibilities are an important goal to achieve.
K29	Communication delays and documentation duties hamper responsiveness.
K30	Business understanding in IT is valued more than technical specialization.
K31	Service provider coordination is a key complexity factor.
K32	ITSM frameworks follow ITIL but lack agile integration.
K33	Satisfaction is assessed through subjective formats like retrospectives and supplier ratings.
K34	Time-to-market and security often conflict in DevOps environments.
K35	Availability metrics may not reflect true user experience.
K36	Transactions are monitored with visual dashboards and escalation rules.
K37	Dynamic metric selection and cross-system aggregation are missing.
K38	Regulatory compliance is increasingly outsourced to certified external providers.
K39	Automation practices are underdeveloped, with core functions such as CI/CD, policy enforcement, and incident response largely outsourced.
K40	Automation is sometimes limited to voice-based alerts for outages.
K41	Compatibility is prioritized over innovation in managing legacy systems.
K42	Changes are managed via CAB with escalation paths and rollback strategies.
K43	AI assists with basic classification tasks but lacks deep analysis capabilities.
K44	Resource buffers and partner coordination are used to manage unpredictability.
K45	Complex partner landscapes increase communication and organizational effort.
K46	Socio-technical complexity emerges from legacy, modern IT, and organizational politics.
K47	Regulations like Solvency II, DORA, GDPR create escalating complexity.
K48	Service performance is measured using technical, process, and incident metrics.

K49	Trade-offs exist between testing depth, cost, and agility in DevOps.
K50	Security is increasingly recognized as a strategic value driver linked to financial and regulatory risk, rather than merely a cost center.
K51	Continuous improvement includes retrospectives, feedback, and proactive measures.
K52	KPI ownership and trend-based reporting guide adaptive performance management.
K53	Automation relies on deep architectural understanding and service mapping.
K54	Predictive maintenance uses historical patterns for proactive scaling.
K55	Automation adds complexity, maintenance needs, and can hit cost ceilings.
K56	Regulatory handling is partially automated but not end-to-end.
K57	Legacy is modernized via shadow systems and functional re-evaluation.
K58	Change management enforces governance via KPIs and automation.
K59	ITSM maturity begins with Incidents, evolves through KPIs and training.
K60	Tools are evaluated based on modifiability and closeness to standards.
K61	Organizational learning is fostered by transparency and social pressure.
K62	Complexity is understood through feedback loops and systemic interrelations.
K63	Service architecture is centralized by headquarters, reducing local autonomy.
K64	Architecture complexity is shaped by volume, granularity, and service visibility.
K65	Incidents and Availability are central metrics with root cause reviews.
K66	Root cause is often a management narrative; true insight lies in lessons learned.
K67	Monitoring spans strategic to operational layers, hindered by log diversity.
K68	Logging detail is increased during incidents, balancing data size and insight.
K69	Automation without stable foundations leads to false-positives and control loss.
K70	Emerging RegTech tools automate compliance mapping and evidence gathering.
K71	Legacy is purpose-driven, not outdated.
K72	Legacy must be defined clearly and phased out via controlled cycles.
K73	Architecture transformation by slicing along business domains rather than data entities, shifting modularization strategy.
K74	Global change procedures slow down delivery and reduce quality.

K75	Regulatory audits consume resources; investment in resilience is more effective.
K76	Neural networks reduce false-positives in monitoring environments.
K77	Asset management and SIAM data quality are critical for effective control.
K78	Predictive maintenance often relies on heuristics and runtime thresholds.
K79	Service integration with security as future objective, anchored in established standards.

## Appendix B: Interview Guide — Round 1 (English)

*This section represents a translation of the original German interview guide into English.*

### 1. Opening Section (5 min)

#### Greeting and consent

Thank you for taking the time for this conversation. I'm studying how financial institutions manage their complex IT systems, with a particular focus on service management, monitoring, automation, and modernization. Your insights will help me better understand real-world practices and validate assumptions from my research.

An essential part of my investigation also concerns non-deterministic behavior and dynamic interactions in such environments—situations where system behavior is unpredictable or hard to reproduce.

Please note that this interview will be [recorded / transcribed], but all data will be anonymized. You may skip any question or end the conversation at any time.

#### Background and role

##### Questions

1. Could you briefly describe your role and your main responsibilities in the company?
2. How long have you worked in financial IT or related fields?
3. Which ITSM areas are you most involved with (e.g., incident response, regulatory compliance, release management, operations)?

## 2. Overall Complexity in Financial IT Systems (5–10 min)

These questions warm up understanding of perceived complexity before linking to specific hypotheses.

### 1) Perception of complexity **Opening prompt**

How would you describe the complexity of your institution's current IT landscape? What are the main drivers (e.g., regulatory, technological, organizational)?

#### **Follow-ups**

- Which factors contribute most (technological, regulatory, organizational)?
- Have these complexity drivers changed over time?

### 2) Challenges and strategies **Opening prompt**

What challenges arise when managing services in this complex environment, and how do you address them (e.g., ITIL, DevOps, internal structures)?

#### **Follow-ups**

- Which strategies or frameworks have proven effective (e.g., ITIL adaptations, SRE, DevOps, SIAM)?
- How are responsibilities distributed across teams or departments?

## 3. Measuring Success and Effectiveness (H1) (5–10 min)

### 1) Current metrics **Opening prompt**

Which KPIs or metrics does your institution use to assess service-management success? Do these go beyond technical aspects (learning, user experience)?

#### **Follow-ups**

- Mostly technical, or also broader indicators (customer experience, continuous improvement, operational risk, knowledge management)?
- Examples: customer satisfaction, NPS, employee experience; post-incident review frequency/quality, team learning cycles; documentation quality/freshness, use of knowledge bases.

### 2) Learning-oriented measures **Opening prompt**

Do you use continuous-improvement and experience-based metrics (e.g., post-incident review frequency, learning velocity; XLAs, customer satisfaction)? If so, how?

#### **Follow-ups**

- What challenges arise when introducing such comprehensive metrics?

**3) Trade-offs when adding new metrics Opening prompt**

Do resource, time, or complexity trade-offs occur when adding broader metrics to capture effectiveness holistically?

**Follow-ups**

- Mechanisms to reflect complex-system dynamics (cascading effects, non-linear follow-ons)?
- Unpredictable or hard-to-explain behavior despite collected metrics?
- Auditor/regulator views on holistic assessment?

**4. Monitoring and Automation (H2/H3) (10–15 min)****1) Monitoring tools and practices Opening prompt**

Which monitoring solutions are in use, and how do they support different stakeholders (operations, compliance, business)?

**Follow-ups**

- Multi-layered monitoring (real-time telemetry, role-based dashboards, event-driven alerts) or static/siloed?
- Stakeholder-specific dashboards and metrics?
- Improvements in early detection and incident management?
- Same action, different outcomes at different times?
- Monitoring of interdependencies across systems?

**2) Adaptive monitoring Opening prompt**

Do you use adaptive monitoring (e.g., dynamic SLOs, anomaly detection, resilience engineering, predictive maintenance, workload rebalancing)? How does it help amid unpredictable behavior?

**Follow-ups**

- Have these methods improved service quality?
- Practical implementation challenges?
- Patterns that emerge only gradually over time?

## 5. Automation (H4) (5–10 min)

### 1) Automation in day-to-day workflows Opening prompt

What role does automation play in daily service processes, and which tools are integrated into service management?

#### Follow-ups

- Compliance/security checks embedded (“policy as code”)?
- Impact on release speed, operational risk, audit readiness?

### 2) Benefits and limits Opening prompt

Have you observed concrete benefits from monitoring and automation? Any concerns (black-box alerts, over-automation, regulatory criticism)?

#### Follow-ups

- Over-automation, opaque decisions, AI false-positives?
- Auditor/regulator responses?
- Fallback processes if automation fails?

## 6. Legacy Systems and Modernization (H5) (5–10 min)

Older IT systems are often technically outdated yet still used because they support core processes. They pose challenges for integration, maintenance, and modernization.

### 1) Scope of legacy systems Opening prompt

What importance do legacy systems have in your IT landscape, and what challenges exist in integrating or replacing them? How do you define a “legacy system”?

#### Follow-ups

- Which core processes or business areas rely most heavily on them?

### 2) Modernization approaches Opening prompt

Does your institution modernize legacy systems incrementally (continuous improvement) or via large-scale transformations? What has your experience been?

#### Follow-ups

- Incremental (strangler pattern, API encapsulation) vs. big-bang migration?
- Challenges encountered (technical, cultural, regulatory)?

**3) Managing technical debt long-term Opening prompt**

Is modernization viewed as a continuous initiative or a one-off major project?

**Follow-ups**

- Differences in outcomes, risk reduction, stability?
- Success stories or lessons learned from stepwise replacement?

**7. Closing Reflection and Open Discussion (5–10 min)****1) Outlook and gaps Opening prompt**

Which trends or technologies will shape service management in complex financial IT environments? Where are the biggest gaps between practice and ideal?

**Follow-ups**

- AI governance, digital twins, zero trust becoming standard?
- Largest disparities between ideal strategies and day-to-day work?
- Managing predictable routines vs. uncertainty?
- Sufficiency of tools/frameworks for emergent or unpredictable behavior?

**2) Advice and takeaways Opening prompt**

Based on your experience, what would you recommend to peers for handling complexity and regulatory requirements?

**3) Closing Opening prompt**

Is there anything we haven't discussed that is relevant for successful service management in complex financial environments?

**Appendix C: Interview Guide — Round 2 (English)**

*This section represents a translation of the original German interview guide into English.*

**1. Opening Section (5 min)****Greeting and consent**

Thank you for taking the time for this conversation. I'm studying how financial institutions manage their complex IT systems, especially regarding service management, monitoring, automation, and modernization. Your insights will help me better understand real-world practices and validate assumptions from my research.

An essential part of my investigation also concerns non-deterministic behavior and dynamic interactions—that is, situations where system behavior is unpredictable or hard to reproduce.

Please note that this interview will be [recorded / transcribed], but all data will be anonymized. You may skip any question or end the conversation at any time.

## Background and role

### Questions

1. Could you briefly describe your role and your main responsibilities in the company?
2. How long have you worked in financial IT or related fields?
3. Which ITSM areas are you most involved with (e.g., incident response, regulatory compliance, release management, operations)?

## 2. Overall Complexity in Financial IT Systems (5–10 min)

These questions capture your perspective on complexity, focusing on causes and control strategies.

### 1) Perception of complexity Opening prompt

How would you rate the overall complexity of your company's current IT system landscape—high, medium, or low?

#### Follow-ups

- Which drivers (technological, regulatory, organizational) have the strongest impact?
- How have these drivers evolved in recent years (strongly increased, unchanged, decreased)?

### 2) Challenges and strategies Opening prompt

What concrete challenges arise from steering and controlling IT services in such complex environments?

#### Follow-ups

- Examples of approaches or strategies that proved effective or less effective (e.g., ITIL adaptations, DevOps/SRE, internal governance structures)?
- Overall success of your current complexity-management strategies (good, medium, poor)?

### 3. Measuring Success and Effectiveness (H1) (5–10 min)

#### 1) Current metrics Opening prompt

Which KPIs or metrics does your institution use to assess service-management success? Could you briefly rate them (good, medium, poor)?

#### Follow-ups

- Which go beyond technical measures? (User experience—customer satisfaction, NPS, employee experience; continuous improvement—frequency/quality of post-incident reviews, team learning cycles; operational risk; knowledge management — documentation quality/freshness, use of knowledge bases.)
- Concrete example of measuring user satisfaction or continuous improvement; how do you assess its explanatory power?

#### 2) Goal conflicts when introducing new metrics Opening prompt

Do you perceive goal conflicts (e.g., resource allocation, complexity) when introducing broader metrics? How strong is this conflict (manageable, moderate, problematic)?

#### Follow-ups

- Can current metrics capture unexpected, non-linear effects (cascading, hard-to-trace follow-on events)?
- Examples where predictive power was limited; how was it addressed?

### 4. Monitoring and Automation (H2/H3) (10–15 min)

#### 1) Monitoring tools and practices Opening prompt

Which monitoring solutions do you currently use, and which stakeholders (operations, compliance, management) benefit most?

#### Follow-ups

- Connected, multi-layered monitoring (real-time telemetry, role-based dashboards, event-driven alerts) or static/siloed?
- Central facilities such as a NOC or comparable 24/7 monitoring/coordination?
- Overall effectiveness (high / medium / low)?
- Stakeholder-specific dashboards and metrics?
- Improvements in early detection and incident management?
- Same action, different outcomes at different times?
- Monitoring solutions that capture interdependencies across systems?

## 2) Adaptive monitoring **Opening prompt**

To what extent do you use adaptive practices (e.g., dynamic SLOs, anomaly detection, resilience engineering, predictive maintenance) to respond to unpredictable behavior?

### Follow-ups

- Noticeable improvement in service quality (significantly / somewhat / unchanged)?
- Temporal patterns or gradually emerging issues—how are they handled? Practical implementation challenges?
- Ability to detect/respond early to dynamic changes (high / medium / low)?
- Influence of hierarchical reporting on decision quality in complex service processes?

## 5. Automation (H4) (5–10 min)

### 1) Automation in day-to-day workflows **Opening prompt**

Which automation strategies are you using in service management, and which tools do you use?

### Follow-ups

- RegTech use (automated checks, control processes, audit dashboards; deletion of personal data; AML checks; DLP)?
- Compliance/governance/security checks embedded in automated processes (“policy as code”)?
- Concrete positive effects (faster releases, fewer compliance incidents, better audit readiness)?
- Impact on release speed, operational risk, audit readiness?
- Challenges or negative effects (“black box” issues, increased complexity)?

### 2) Benefits and limits **Opening prompt**

Overall benefit of current service-process automation for efficiency (good, medium, poor)?

### Follow-ups

- Concerns about over-automation, opaque decisions, AI false-positives?
- Auditor/regulator assessments (positive, neutral, critical)?
- Fallback processes if an automated system fails?

**3) AIOps (Artificial Intelligence for IT Operations) Opening prompt**

Do you use AIOps approaches—AI-based analytics for incident detection, root-cause analysis, or response automation?

**Follow-ups**

- Covered use cases (anomaly detection, alert correlation, automated tuning)?
- Added value for operational control (high, medium, low)?
- Status: piloting, production use, or planned?

**6. Legacy Systems and Modernization (H5) (5–10 min)**

Older IT systems are often technically outdated yet still used because they support core business processes; they pose challenges for integration, maintenance, and modernization.

**1) Scope of legacy systems Opening prompt**

What role do legacy systems currently play in your IT landscape? How large are the resulting challenges in maintenance, integration, or modernization (large, medium, small)?

**Follow-ups**

- Which core processes or business areas rely most heavily on them?
- Recent issues due to legacy systems (integration problems, security incidents, increased maintenance effort)?

**2) Modernization approaches Opening prompt**

Which approach dominates: continuous, incremental modernization or extensive, one-off transformation projects?

**Follow-ups**

- Incremental approaches (strangler pattern, API encapsulation) or big-bang migrations?
- Stepwise modernization while the old system runs in the background—how successful (good, medium, poor)?
- Challenges encountered (technical, cultural, regulatory)?

**3) Managing technical debt long-term Opening prompt**

How does change management typically work for modifications to existing (especially older) systems?

**Follow-ups**

- Formal CABs or other bodies assessing/approving changes?
- Roles/departments typically involved (IT, risk, compliance, business)?
- Coordination quality between technical and business stakeholders (good, medium, poor)?

#### 4) **Microservices** **Opening prompt**

To what extent do you pursue a microservices approach when replacing or evolving legacy systems (decomposing monoliths into smaller, loosely coupled units)?

##### **Follow-ups**

- Experience regarding governance, deployment complexity, team structure?
- Decision-making: central (architectural guidelines) or decentral (teams)?
- Examples where the shift to microservices went particularly well—or was challenging?

### 7. **Closing Reflection and Open Discussion (5–10 min)**

#### 1) **Outlook and gaps** **Opening prompt**

Which trends or technologies will shape service management in complex financial IT environments? Where are the biggest gaps between practice and ideal?

##### **Follow-ups**

- AI governance, digital twins, or zero trust becoming standard?
- Largest disparities between ideal strategies and day-to-day operations?
- Managing predictable routines vs. uncertainty?
- Sufficiency of current tools/frameworks for emergent or unpredictable behavior?

#### 2) **Advice and takeaways** **Opening prompt**

Do new implementations—modern tools, architectures, platforms—tend to reduce or increase complexity in your organization?

##### **Follow-ups**

- Attention to new dependencies or control challenges when introducing solutions?
- Strategies/governance rules to detect and minimize hidden complexity or unintended interactions?
- Example where a new technology caused unexpected complexity—or sustainably reduced problems?

### 3) Closing Opening prompt

Is there anything we haven't discussed that is relevant for successful service management in complex financial environments?

# Bibliography

- [1] Syed Imran Abbas and Ankit Garg. “AIOps in DevOps: Leveraging Artificial Intelligence for Operations and Monitoring”. In: *2024 3rd International Conference on Sentiment Analysis and Deep Learning (ICSADL)*. 2024, pp. 64–70. DOI: 10.1109/ICSADL61749.2024.00016.
- [2] Ujué Agudo et al. “The impact of AI errors in a human-in-the-loop process”. In: *Cognitive Research: Principles and Implications* 9.1 (Jan. 2024), p. 1. ISSN: 2365-7464. DOI: 10.1186/s41235-023-00529-3.
- [3] Rainer Alt, Roman Beck, and Martin T. Smits. “FinTech and the transformation of the financial industry”. In: *Electronic Markets* 28.3 (Aug. 2018), pp. 235–243. ISSN: 1422-8890. DOI: 10.1007/s12525-018-0310-9.
- [4] Philip W. Anderson. *The Theory of Superconductivity in the High-Tc Cuprates*. Series: Cambridge Lecture Notes in Physics. Cambridge, UK: Cambridge University Press, 1999. ISBN: 978-0521462457.
- [5] Anca Apostu, Emanuil Rednic, and Florina Puican. “Modeling Cloud Architecture in Banking Systems”. In: *Procedia Economics and Finance* 3 (2012). International Conference Emerging Markets Queries in Finance and Business, Petru Maior University of Tîrgu-Mures, ROMANIA, October 24th - 27th, 2012, pp. 543–548. ISSN: 2212-5671. DOI: 10.1016/S2212-5671(12)00193-1.
- [6] Seyed Mohammad Asadzadeh, Hadi Maleki, and Mehrab Tanhaeean. “A resilience engineering-based approach to improving service reliability in maintenance organizations”. In: *International Journal of System Assurance Engineering and Management* 11.5 (Oct. 2020), pp. 909–922. ISSN: 0976-4348. DOI: 10.1007/s13198-020-01015-5.
- [7] W. Ross Ashby. *An Introduction to Cybernetics*. London: Chapman & Hall, 1956. ISBN: 9783518276341.
- [8] Karl Åström et al. *Control of Complex Systems*. Springer London, 2000. ISBN: 9781852333249. DOI: 10.1007/978-1-4471-0349-3.
- [9] AXELOS Limited. *ITIL Foundation: ITIL 4 Edition*. Official ITIL 4 Foundation Guide. London, UK: TSO (The Stationery Office), 2019. ISBN: 9780113316076. URL: <https://www.axelos.com/certifications/itil-certifications/itil-4-foundation>.

- [10] Fikri Aydemir and Fatih Başgıftçi. “Building a Performance Efficient Core Banking System Based on the Microservices Architecture”. In: *Journal of Grid Computing* 20.4 (Nov. 2022), p. 37. ISSN: 1572-9184. DOI: 10.1007/s10723-022-09624-z.
- [11] Kamran Ayub and Roushdy AlShawa. “A New Intelligent Event Correlation paradigm in HetNets: A Case Study of ServiceNow’s AIOps Capabilities”. In: *2024 IEEE International Conference on Internet of Things and Intelligence Systems (IoTaIS)*. 2024, pp. 26–31. DOI: 10.1109/IoTaIS64014.2024.10799287.
- [12] Albert-László Barabási. *Linked: The New Science of Networks*. Cambridge, MA: Perseus Publishing, 2002.
- [13] Basel Committee on Banking Supervision. *Basel III: A Global Regulatory Framework for More Resilient Banks and Banking Systems*. Revised version. June 2011. URL: <https://www.bis.org/publ/bcbs189.htm>.
- [14] Ali Basiri et al. “Chaos Engineering”. In: *IEEE Software* 33.3 (2016), pp. 35–41. DOI: 10.1109/MS.2016.60.
- [15] Stafford Beer. *Brain of the Firm*. London: Allen Lane, 1972. ISBN: 9780471948391.
- [16] Stafford Beer. “The Viable System Model: Its Provenance, Development, Methodology and Pathology”. In: *Journal of the Operational Research Society* 35.1 (1984), pp. 7–25. DOI: 10.1057/jors.1984.2.
- [17] Nasim Beigi-Mohammadi et al. “Adaptive service management for cloud applications using overlay networks”. In: *2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*. 2017, pp. 386–392. DOI: 10.23919/INM.2017.7987302.
- [18] Chafika Benzaid and Tarik Taleb. “AI-Driven Zero Touch Network and Service Management in 5G and Beyond: Challenges and Research Directions”. In: *IEEE Network* 34.2 (2020), pp. 186–194. DOI: 10.1109/MNET.001.1900252.
- [19] Egon Berghout and Rob Fijneman. “Auditing Complexity”. In: *Advanced Digital Auditing: Theory and Practice of Auditing Complex Information Systems and Technologies*. Ed. by Egon Berghout et al. Cham: Springer International Publishing, 2023, pp. 9–14. ISBN: 978-3-031-11089-4. DOI: 10.1007/978-3-031-11089-4\_2.
- [20] Alexander Berman, Marcelo Cano-Kollmann, and Ram Mudambi. “Innovation and entrepreneurial ecosystems: fintech in the financial services industry”. In: *Review of Managerial Science* 16.1 (Jan. 2022), pp. 45–64. ISSN: 1863-6691. DOI: 10.1007/s11846-020-00435-8.
- [21] Betsy Beyer et al. *Site Reliability Engineering: How Google Runs Production Systems*. Sebastopol, CA: O’Reilly Media, 2016. ISBN: 9781491929124.
- [22] Nino Boccarda. *Modeling Complex Systems*. New York: Springer Science & Business Media, 2010. ISBN: 978-1-4419-6561-5. DOI: 10.1007/978-1-4419-6562-2.
- [23] Alexander Bogner, Beate Littig, and Wolfgang Menz. *Interviewing Experts*. Palgrave Macmillan, 2009.

- [24] Justus Bogner et al. “Limiting technical debt with maintainability assurance: an industry survey on used techniques and differences with service- and microservice-based systems”. In: *Proceedings of the 2018 International Conference on Technical Debt*. TechDebt '18. Gothenburg, Sweden: Association for Computing Machinery, 2018, pp. 125–133. ISBN: 9781450357135. DOI: 10.1145/3194164.3194166.
- [25] Jean-Louis Boulanger, ed. *Formal Methods Applied to Industrial Complex Systems*. London: Springer, 2014. ISBN: 9781119004707. DOI: 10.1002/9781119004707.
- [26] Virginia Braun and Victoria Clarke. “Using thematic analysis in psychology”. In: *Qualitative Research in Psychology* 3.2 (2006), pp. 77–101. DOI: 10.1191/1478088706qp0630a.
- [27] California State Legislature. *California Consumer Privacy Act of 2018 (CCPA), California Civil Code §§ 1798.100 - 1798.199.100*. Enacted in 2018, amended by the California Privacy Rights Act (CPRA) in 2020. 2018. URL: [https://leginfo.ca.gov/faces/codes\\_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5](https://leginfo.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5).
- [28] C.N. Calvano and P. John. “Systems engineering in an age of complexity”. In: *IEEE Engineering Management Review* 32.4 (2004), pp. 29–38. DOI: 10.1109/EMR.2004.25134.
- [29] Avyay Casheekar et al. “A contemporary review on chatbots, AI-powered virtual conversational agents, ChatGPT: Applications, open challenges and future research directions”. In: *Computer Science Review* 52 (2024), p. 100632. ISSN: 1574-0137. DOI: 10.1016/j.cosrev.2024.100632.
- [30] Ni-Bin Chang, Adriano Pires, and Graça Martinho. “Resilience and adaptive capacity of complex systems”. In: *Journal of Infrastructure Systems* 19.3 (2013), pp. 223–234.
- [31] Lianping Chen. “Continuous Delivery: Huge Benefits, but Challenges Too”. In: *IEEE Software* 32.2 (2015), pp. 50–54. DOI: 10.1109/MS.2015.27.
- [32] Dimitrios Christopoulos. “Peer esteem snowballing: A methodology for expert selection”. In: *Social Networks* 29.1 (2007), pp. 43–55.
- [33] Orges Cico et al. “Exploring the intersection between software industry and Software Engineering education - A systematic mapping of Software Engineering Trends”. In: *Journal of Systems and Software* 172 (2021), p. 110736. ISSN: 0164-1212. DOI: 10.1016/j.jss.2020.110736.
- [34] Competition and Markets Authority (CMA). *The Retail Banking Market Investigation Order 2017 (CMA Order) - Implementing Open Banking in the UK*. Legal framework for Open Banking in the UK, issued by the CMA. 2017. URL: <https://www.gov.uk/government/publications/retail-banking-market-investigation-order-2017>.

- [35] Control System Cybersecurity Association International (CS)<sup>2</sup>AI and KPMG International. *Control System Cybersecurity Annual Report 2024*. (CS)<sup>2</sup>AI and KPMG International, 2024.
- [36] Nancy J. Cooke and Janet E. McDonald. “A formal methodology for acquiring and representing expert knowledge”. In: *Journal of Human Factors* 28.4 (1986), pp. 471–482.
- [37] Priyanshi David, Mohit Kumar Kushwaha, and G. Suseela. “DevSecOps in Finance: Strengthening the Security Model of Applications”. In: *2024 4th International Conference on Data Engineering and Communication Systems (ICDECS)*. 2024, pp. 1–6. DOI: 10.1109/ICDECS59733.2023.10502917.
- [38] Aniket Deshpande. “Regulatory Compliance and AI: Navigating the Legal and Regulatory Challenges of AI in Finance”. In: *2024 International Conference on Knowledge Engineering and Communication Systems (ICKECS)*. Vol. 1. 2024, pp. 1–5. DOI: 10.1109/ICKECS61492.2024.10616752.
- [39] Yixin Diao and Larisa Shwartz. “Building Automated Data Driven Systems for IT Service Management”. In: *Journal of Network and Systems Management* 25.4 (Oct. 2017), pp. 848–883. ISSN: 1573-7705. DOI: 10.1007/s10922-017-9430-3.
- [40] Howard Eisner. *Managing Complex Systems: Thinking outside the Box*. Wiley-Interscience, Oct. 2005, pp. 1–201. ISBN: 9780471690061. DOI: 10.1002/0471745499.
- [41] Lars Eriksson. “Knowledge acquisition techniques in expert systems”. In: *AI Review* 6.1 (1992), pp. 3–30.
- [42] European Parliament and Council of the European Union. *Directive (EU) 2014/65 of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (MiFID II)*. Official Journal of the European Union, L 173, 12 June 2014, pp. 349-496. 2014. URL: <https://eur-lex.europa.eu/eli/dir/2014/65/oj>.
- [43] European Parliament and Council of the European Union. *Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (Payment Services Directive 2)*. Official Journal of the European Union, L 337, 23 December 2015, pp. 35-127. 2015. URL: <https://eur-lex.europa.eu/eli/dir/2015/2366/oj>.
- [44] European Parliament and Council of the European Union. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. Official Journal of the European Union, L 119, 4 May 2016, pp. 1-88. 2016. URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>.

- [45] European Union. *Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II)*. Official Journal of the European Union, L 335, 17.12.2009, p. 1–155. 2009. URL: <https://eur-lex.europa.eu/eli/dir/2009/138/oj/eng>.
- [46] European Union. *Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014, and (EU) 2016/1011*. Official Journal of the European Union, L 333, 27.12.2022, p. 1–54. 2022.
- [47] Jennifer Fereday and Eimear Muir-Cochrane. “Demonstrating Rigor Using Thematic Analysis: A Hybrid Approach of Inductive and Deductive Coding and Theme Development”. In: *International Journal of Qualitative Methods* 5.1 (2006), pp. 80–92. DOI: 10.1177/160940690600500107.
- [48] Elena Gibadullina, Elena Viskova, and Sergey Stepanov. “Automated Service Configuration Management in IP/MPLS Networks”. In: *2022 International Conference on Modern Network Technologies (MoNeTec)*. 2022, pp. 1–5. DOI: 10.1109/MoNeTec55448.2022.9960765.
- [49] Marius Goldberg, Axel Kieninger, and Hansjörg Fromm. “Organizational Models for the Multi-sourcing Service Integration and Management Function”. In: *2014 IEEE 16th Conference on Business Informatics*. Vol. 2. 2014, pp. 101–107. DOI: 10.1109/CBI.2014.43.
- [50] “Guest Editorial Special Issue on Complex Systems in Finance and Economics”. In: *IEEE Systems Journal* 12.2 (2018), pp. 1087–1089. DOI: 10.1109/JSYST.2018.2817978.
- [51] Jack Laurie Harris. “Bridging the gap between ‘Fin’ and ‘Tech’: The role of accelerator networks in emerging FinTech entrepreneurial ecosystems”. In: *Geoforum* 122 (2021), pp. 174–182. ISSN: 0016-7185. DOI: 10.1016/j.geoforum.2021.04.010.
- [52] K. Herrmann, G. Muhl, and K. Geihs. “Self management: the solution to complexity or just another problem?” In: *IEEE Distributed Systems Online* 6.1 (2005). DOI: 10.1109/MDSO.2005.3.
- [53] John H. Holland. “Complex Adaptive Systems”. In: *Daedalus* 121.1 (1992), pp. 17–30.
- [54] Erik Hollnagel, David D. Woods, and Nancy G. Leveson, eds. *Resilience Engineering: Concepts and Precepts*. Aldershot, UK: Ashgate Publishing, 2006.
- [55] S. E. Hove and Bente Anda. “Experiences from conducting semi-structured interviews in empirical software engineering research”. In: *Empirical Software Engineering* 10.4 (2005), pp. 311–341.

- [56] KPMG International. *Intelligent Banking: A Blueprint for Creating Value through AI-Driven Transformation*. KPMG International, 2025.
- [57] International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC). *ISO/IEC 20000-1:2018 - Information Technology - Service Management - Part 1: Service Management System Requirements*. Tech. rep. Latest edition of ISO/IEC 20000-1. Geneva, Switzerland, 2018. URL: <https://www.iso.org/standard/70636.html>.
- [58] ISACA. *COBIT 2019 Framework: Governance and Management Objectives*. Latest version of COBIT framework. Schaumburg, IL, USA: Information Systems Audit and Control Association (ISACA), 2018. ISBN: 978-1604207286. URL: <https://www.isaca.org/resources/cobit>.
- [59] Haidar Jabbar, Samir Al-Janabi, and Francis Syms. “AI-Integrated Cyber Security Risk Management Framework for IT Projects”. In: *2024 International Jordanian Cybersecurity Conference (IJCC)*. 2024, pp. 76–81. DOI: 10.1109/IJCC64742.2024.10847294.
- [60] T. Khraisha. *Financial Data Engineering: Design and Build Data-Driven Financial Products*. O’Reilly Media, 2024. ISBN: 9781098159955.
- [61] Hee-Gon Kim, Jae-Hyoung Yoo, and James Won-Ki Hong. “AI-based Network Function Virtualization Orchestration”. In: *NOMS 2024-2024 IEEE Network Operations and Management Symposium*. 2024, pp. 1–5. DOI: 10.1109/NOMS59830.2024.10575048.
- [62] Barbara Kitchenham and Stuart Charters. *Guidelines for performing systematic literature reviews in software engineering*. Tech. rep. EBSE-2007-01. Keele University, 2007.
- [63] Khoa Lam et al. “A Framework for Assurance Audits of Algorithmic Systems”. In: *Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency*. FAccT ’24. Rio de Janeiro, Brazil: Association for Computing Machinery, 2024, pp. 1078–1092. ISBN: 9798400704505. DOI: 10.1145/3630106.3658957.
- [64] Jiaxin Li et al. “Performance Bug Analysis and Detection for Distributed Storage and Computing Systems”. In: *ACM Trans. Storage* 19.3 (June 2023). ISSN: 1553-3077. DOI: 10.1145/3580281.
- [65] Ming Li and Carol Smidts. “A framework for comparing traditional and complex systems”. In: *Reliability Engineering & System Safety* 80.2 (2003), pp. 133–144.
- [66] Kristian Lindgren. *Information Theory for Complex Systems: An Information Perspective on Complexity in Dynamical Systems and Statistical Mechanics*. Understanding complex systems. Springer Berlin, 2024. ISBN: 9783662683729. DOI: 10.1007/978-3-662-68214-2.

- [67] Yang-Yu Liu and Albert-László Barabási. “Control Principles of Complex Networks”. In: *CoRR* abs/1508.05384 (2015). DOI: 10.48550/arXiv.1508.05384. arXiv: 1508.05384.
- [68] Yi Liu, Jiawen Peng, and Zhihao Yu. “Big Data Platform Architecture under The Background of Financial Technology: In The Insurance Industry As An Example”. In: *Proceedings of the 2018 International Conference on Big Data Engineering and Technology*. BDET '18. Chengdu, China: Association for Computing Machinery, 2018, pp. 31–35. ISBN: 9781450365826. DOI: 10.1145/3297730.3297743.
- [69] J. A. Tenreiro Machado and António M. Lopes. *Symmetry in Complex Systems*. Cham: Springer, 2020. ISBN: 978-3-03936-894-5. DOI: 10.3390/books978-3-03936-895-2.
- [70] Don MacLean and Ryad Titah. “Implementation and impacts of IT Service Management in the IT function”. In: *International Journal of Information Management* 70 (2023), p. 102628. ISSN: 0268-4012. DOI: 10.1016/j.ijinfomgt.2023.102628.
- [71] Abhishek Mahalle, Jianming Yong, and Xiaohui Tao. “ITIL Processes to Control Operational Risk in Cloud Architecture Infrastructure for Banking and Financial Services Industry”. In: *2018 5th International Conference on Behavioral, Economic, and Socio-Cultural Computing (BESC)*. 2018, pp. 197–200. DOI: 10.1109/BESC.2018.8697294.
- [72] S. Mahdavi-Hezavehi, P. Avgeriou, and D. Weyns. “Chapter 3 - A Classification Framework of Uncertainty in Architecture-Based Self-Adaptive Systems With Multiple Quality Requirements”. In: *Managing Trade-Offs in Adaptable Software Architectures*. Ed. by Ivan Mistrik et al. Boston: Morgan Kaufmann, 2017, pp. 45–77. ISBN: 978-0-12-802855-1. DOI: 10.1016/B978-0-12-802855-1.00003-4.
- [73] Moinak Maiti and Uttam Ghosh. “Next-Generation Internet of Things in Fintech Ecosystem”. In: *IEEE Internet of Things Journal* 10.3 (2023), pp. 2104–2111. DOI: 10.1109/JIOT.2021.3063494.
- [74] C Manjula Devi et al. “Next-Generation Anomaly Detection Framework Leveraging Artificial Intelligence for Proactive Credit Card Fraud Prevention and Risk Management”. In: *2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT)*. 2024, pp. 1–6. DOI: 10.1109/ICCCNT61001.2024.10725285.
- [75] Abdelrahman Mayar, Mohamed Al-Hussein, and Ahmed Bouferguene. “Stability and Resilience—A Systematic Approach”. In: *Buildings* 12.8 (2022), p. 1242. DOI: 10.3390/buildings12081242.
- [76] Cheikh Saliou Mbacke Babou et al. “AI-Driven Automation for Optimal Edge Cluster Network Management”. In: *IEEE INFOCOM 2024 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. 2024, pp. 1–6. DOI: 10.1109/INFOCOMWKSHPS61880.2024.10620722.

- [77] Ines Mergel, Noella Edelmann, and Nathalie Haug. “Conducting expert interviews in public administration research”. In: *International Journal of Public Administration* 42.5 (2019), pp. 392–402.
- [78] Jamil Mina. *Bringing reliability to banking services: a new twist on Site Reliability Engineering*. Accessed: 2025-04-12. June 2021. URL: <https://www.redhat.com/en/blog/bringing-reliability-banking-services-new-twist-site-reliability-engineering>.
- [79] Nawazish Mirza et al. “Safeguarding FinTech innovations with machine learning: Comparative assessment of various approaches”. In: *Research in International Business and Finance* 66 (2023), p. 102009. ISSN: 0275-5319. DOI: 10.1016/j.ribaf.2023.102009.
- [80] Melanie Mitchell and Zoltan Toroczkai. “Complexity: A Guided Tour”. In: *Physics Today* 63 (Feb. 2010), pp. 47–. DOI: 10.1063/1.3326990.
- [81] Saurabh Mittal, Saikou Diallo, and Andreas Tolk. *Emergent Behavior in Complex Systems Engineering: A Modeling and Simulation Approach*. John Wiley & Sons, Apr. 2018. ISBN: 978-1-119-37893-8.
- [82] David Moriarty, ed. *Preface*. Academic Press, 2023. ISBN: 978-0-323-91609-7. DOI: 10.1016/B978-0-323-91609-7.15003-6.
- [83] Michael Muhlmeyer, Shaurya Agarwal, and Archie J. Huang. “Modeling Social Contagion and Information Diffusion in Complex Socio-Technical Systems”. In: *IEEE Systems Journal* 14.4 (2020), pp. 5187–5198. DOI: 10.1109/JSYST.2020.2993542.
- [84] Humza Naseer et al. “Enabling cybersecurity incident response agility through dynamic capabilities: the role of real-time analytics”. In: *European Journal of Information Systems* 33.2 (2024), pp. 200–220. DOI: 10.1080/0960085X.2023.2257168.
- [85] M. E. J. Newman. “Complex Systems: A Survey”. In: *American Journal of Physics* 79.8 (July 2011), pp. 800–810. ISSN: 1943-2909. DOI: 10.1119/1.3590372.
- [86] R. R. Nigmatullin and B. N. Nougmanov. “New Solutions of the Functional Equations and Their Possible Application in Treatment of Complex Systems”. In: *Mathematical Methods in Engineering: Applications in Dynamics of Complex Systems*. Ed. by Kenan Taş, Dumitru Baleanu, and J. A. Tenreiro Machado. Cham: Springer International Publishing, 2019, pp. 3–24. ISBN: 978-3-319-90972-1. DOI: 10.1007/978-3-319-90972-1\_1.
- [87] Raphael Norman-Tenazas et al. “Towards Trustworthy Distributed AI Demand Response”. In: *2024 International Conference on Assured Autonomy (ICAA)*. 2024, pp. 106–109. DOI: 10.1109/ICAA64256.2024.00025.
- [88] Lorelli S. Nowell et al. “Thematic Analysis: Striving to Meet the Trustworthiness Criteria”. In: *International Journal of Qualitative Methods* 16.1 (2017), p. 1609406917733847. DOI: 10.1177/1609406917733847.

- [89] Pawel Pinio, Roman Batko, and Dagmara Lewicka. “Between Theory and Value Transactions: A Multifaceted Exploration of Relevance and Resilience of Decentralised Autonomous Organisations”. In: *Proceedings of the 2024 7th International Conference on Software Engineering and Information Management*. ICSIM '24. Suva, Fiji: Association for Computing Machinery, 2024, pp. 42–48. ISBN: 9798400709197. DOI: 10.1145/3647722.3647729.
- [90] Robert W. Proctor and Trisha Van Zandt. *Human Factors in Simple and Complex Systems, Second Edition*. 2nd. USA: CRC Press, Inc., 2017. ISBN: 1138747513.
- [91] Thomas Puschmann. “Fintech”. In: *Business & Information Systems Engineering* 59.1 (Feb. 2017), pp. 69–76. ISSN: 1867-0202. DOI: 10.1007/s12599-017-0464-6.
- [92] Naila Iqbal Qureshi et al. “Ethical Considerations of AI in Financial Services: Privacy, Bias, and Algorithmic Transparency”. In: *2024 International Conference on Knowledge Engineering and Communication Systems (ICKECS)*. Vol. 1. 2024, pp. 1–6. DOI: 10.1109/ICKECS61492.2024.10616483.
- [93] Petar Radanliev et al. “Epistemological Equation for Analysing Uncontrollable States in Complex Systems: Quantifying Cyber Risks from the Internet of Things”. In: *The Review of Socionetwork Strategies* 15.2 (Nov. 2021), pp. 381–411. ISSN: 1867-3236. DOI: 10.1007/s12626-021-00086-5.
- [94] Donald G. Reinertsen. *The Principles of Product Development Flow: Second Generation Lean Product Development*. Celeritas Publishing, 2009. ISBN: 9781935401001.
- [95] Sergio Rivera, Amro M. Farid, and Kamal Youcef-Toumi. “A multi-agent system transient stability platform for resilient self-healing operation of multiple microgrids”. In: *ISGT 2014*. 2014, pp. 1–5. DOI: 10.1109/ISGT.2014.6816377.
- [96] Daniel Russo et al. “A Meta-Model for Information Systems Quality: A Mixed Study of the Financial Sector”. In: *ACM Trans. Manage. Inf. Syst.* 9.3 (Sept. 2018). ISSN: 2158-656X. DOI: 10.1145/3230713.
- [97] Navin Sabharwal and Gaurav Bhardwaj. “What Is AIOps?” In: *Hands-on AIOps: Best Practices Guide to Implementing AIOps*. Berkeley, CA: Apress, 2022, pp. 1–17. ISBN: 978-1-4842-8267-0. DOI: 10.1007/978-1-4842-8267-0\_1.
- [98] Johnny Saldaña. *Fundamentals of Qualitative Research*. Oxford University Press, 2011.
- [99] Vahid Salehi, Brian Veitch, and Douglas Smith. “Modeling complex socio-technical systems using the FRAM: A literature review”. In: *Human Factors and Ergonomics in Manufacturing & Service Industries* 31.1 (2021), pp. 118–142. DOI: 10.1002/hfm.20874.
- [100] Sergio Scandizzo. *The Validation of Risk Models: A Handbook for Practitioners*. London: Palgrave Macmillan, 2016. ISBN: 978-1-137-43696-2. DOI: 10.1057/9781137436962.

- [101] Daniel Schäfer. “Referenzmodelle des IT-Management”. In: *Lean-Informationstechnik im Finanzdienstleistungssektor: Wege zu Prozess- und Kostenoptimierung mit ITIL & Lean*. Wiesbaden: Springer Fachmedien Wiesbaden, 2015, pp. 19–34. ISBN: 978-3-658-06989-6. DOI: 10.1007/978-3-658-06989-6\_3.
- [102] Shubham Singh, Ajai Gaur, and Deeksha Singh. “Blockchain-Based Governance: Implications for Organizational Boundaries and Structures”. In: *British Journal of Management* 35.4 (2024), pp. 1692–1699. DOI: 10.1111/1467-8551.12784.
- [103] David J. Snowden and Mary E. Boone. “A Leader’s Framework for Decision Making”. In: *Harvard Business Review* 85.11 (2007), pp. 68–76.
- [104] Ian Sommerville et al. “Large-scale complex IT systems”. In: *Commun. ACM* 55.7 (July 2012), pp. 71–77. ISSN: 0001-0782. DOI: 10.1145/2209249.2209268.
- [105] Thomas Sowell. *Knowledge and Decisions*. New York: Basic Books, 1980. ISBN: 9780465037384.
- [106] Anselm Strauss and Juliet Corbin. *Grounded Theory: Grundlagen qualitativer Sozialforschung*. Weinheim: Beltz, 1996.
- [107] Eren Tarak and H. Hakan Kilinc. “DIA4M: A Tool to Streamline DevOps Processes of Distributed Cloud-Native Systems”. In: *2024 9th International Conference on Computer Science and Engineering (UBMK)*. 2024, pp. 1110–1115. DOI: 10.1109/UBMK63289.2024.10773447.
- [108] Ciza Thomas, Rendhir R. Prasad, and Minu Mathew. “Introduction to Complex Systems, Sustainability and Innovation”. In: *Complex Systems, Sustainability and Innovation*. Ed. by Ciza Thomas. Rijeka: IntechOpen, 2016. Chap. 1. DOI: 10.5772/66453.
- [109] S. Thurner, R.A. Hanel, and P. Klimek. *Introduction to the Theory of Complex Systems*. Oxford University Press, 2018. ISBN: 9780191861062.
- [110] Lei Tian and Amandeep Kaur. “Design and Implementation of Financial Service and Management Platform considering Support Vector Machine Algorithm”. In: *Intell. Neuroscience 2022* (Jan. 2022). ISSN: 1687-5265. DOI: 10.1155/2022/7964123.
- [111] Joe Tranquillo. *An Introduction to Complex Systems: Making Sense of a Changing World*. Springer Berlin, Jan. 2019. ISBN: 978-3-030-02588-5. DOI: 10.1007/978-3-030-02589-2.
- [112] Ernesto Troiano et al. “Big Data Platform for Integrated Cyber and Physical Security of Critical Infrastructures for the Financial Sector: Critical Infrastructures as Cyber-Physical Systems”. In: *Proceedings of the 11th International Conference on Management of Digital EcoSystems*. MEDES ’19. Limassol, Cyprus: Association for Computing Machinery, 2020, pp. 262–269. ISBN: 9781450362382. DOI: 10.1145/3297662.3365787.

- [113] Stephen L. Vargo and Robert F. Lusch. “Service-dominant logic: continuing the evolution”. In: *Journal of the Academy of Marketing Science* 36.1 (Mar. 2008), pp. 1–10. ISSN: 1552-7824. DOI: 10.1007/s11747-007-0069-6.
- [114] Ingo Walter. “Universal banking and financial architecture”. In: *The Quarterly Review of Economics and Finance* 52.2 (2012), pp. 114–122. ISSN: 1062-9769. DOI: 10.1016/j.qref.2011.12.007.
- [115] Jane Webster and Richard T. Watson. *Analyzing the past to prepare for the future: Writing a literature review*. Tech. rep. MIS Quarterly, 2002.
- [116] Dewi Yokelson et al. “SOMA: Observability, monitoring, and in situ analytics for exascale applications”. In: *Concurrency and Computation: Practice and Experience* 36.19 (2024), e8141. DOI: 10.1002/cpe.8141.